4/2014

Datenschutz Nachrichten

37. Jahrgang
ISSN 0137-7767
12,00 Euro

Big Data

■ Vom überwachten Bürger zum gläsernen Menschen ■ Auswertung personenbezogener Daten für Strafverfolgung und Gefahrenabwehr ■ Big Data und Mitbestimmung ■ Cloud Computing und Datenschutz ■ Anti-Doping-Kontrollen ■ Bestandsdaten-Auskunftsgesetz ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine

Dienstag, 27. Januar 2015, 18 Uhr
„Das Recht, vergessen zu werden, Informationsfreiheit und Datenschutz”
Diskussionsveranstaltung mit
Sabine Leutheusser-Schnarrenberger, Paul Nemitz, Prof. Dr. Indra Spiecker genannt Döhmann, Prof. Dr. Johannes Caspar, Jan Kottmann,
Diskussionsleitung: Peter Schaar (EAID)
Veranstaltungsort: Europäische Akademie für Informationsfreiheit und Datenschutz
Bismarckallee 46/48, D-14193 Berlin
Um Anmeldung per E-Mail an gf@eaid-berlin.de wird gebeten. Weitere Informationen www.eaid-berlin.de

Sonntag, 01.Februar 2015
Redaktionsschluss DANA 1/2015
Thema: Mobilität/Telematik

Dienstag, 03.Februar 2015, 09:00-17:15 Uhr
Fachtagung Datenschutz in der Medizin
Datenschutz in der Medizin - Update 2015!
Hotel Hafen Hamburg,
http://www.update-bdsg.com/tagung/hamburg/datenschutz-in-der-medizin-update-2015/uebersicht.html

Dienstag, 24. Februar 2015
THM-Datenschutztag 2015.
Themen: Cloud Computing, Datenspionage und Google Glass.
Campus Gießen, Gebäude A 20, Hörsaal 1.36 (1. OG)
Wiesenstraße
Info und Anmeldung: http://www.thm.de/datenschutz/datenschutztag/214-thm-datenschutztag-2015

Freitag, 09. Oktober 2015 – 10. Oktober 2015
DVD-Jahrestagung
Thema: Mobilität und Telematik (Arbeitstitel)

Foto: Uwe Schlick pixelio.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
37. Jahrgang, Heft 4

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Rheingasse 8-10, 53113 Bonn
Tel. 0228-222498
Konto 1900 2187, BLZ 370 501 98, Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Jaqueline Rüdiger
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Rheingasse 8-10, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0)91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, soweit nicht anders gekennzeichnet

Editorial

Liebe Leserinnen und Leser,

Big Data ist ein Heilsversprechen. Krankheiten sollen besser vorhergesagt werden können und die Rettung der Erde durch Energieeinsparmaßnahmen wird beteuert. Manche erhoffen sich zudem das schnelle Geld durch eine Vorhersagbarkeit der Börsenkurse. Big Data ist jedoch auch eine Gefahr für das Individuum. Datenschutzrechte wie das Recht auf Transparenz oder zweckgebundene Verwendung von Daten werden grundlegend infrage gestellt.

Doch was ist eigentlich Big Data? In den meisten Fällen wird Big Data in etwa wie folgt beschrieben: Aus verschiedenen Quellen entstehen große Datensammlungen, die andere Auswertetechniken erfordern und häufig auch neue Zusammenhänge sichtbar werden lassen. Big Data ist zunächst ein Sammeln und Aggregieren von Daten zwecks Sichtbar-Machens neuer Zusammenhänge. Ein wesentliches Problem: Die Zweckbestimmung steht häufig nicht von vornherein fest, sondern ergibt sich vielmehr erst aus dem Ergebnis der Auswertung selbst. Außerdem sind die verwendeten Algorithmen oftmals nicht bekannt; sie werden als Geschäftsgeheimnis gewahrt. Der Einzelne kann die Güte des Algorithmus nicht kontrollieren. Mit Big Data-Anwendungen sind zudem auch sog. „Kontrollstrategien“ umsetzbar. Durch Manipulation eines Objekts sollen positive Ergebnisse erzielt werden. Dies erscheint unkritisch, wenn es um das Beeinflussen einer Produktionsstraße geht. Ethisch fragwürdig wird die Manipulation dann, wenn der Mensch beeinflusst werden soll.

Höchste Zeit, dass die DVD Big Data eine eigene Ausgabe widmet! Der Journalist Peter Welchering verschafft uns in der aktuellen DANA einen Überblick über die Möglichkeiten und Risiken von Big Data-Anwendungen. Barbara Körffer widmet sich dem Thema Big Data hinsichtlich Auswertungen für Strafverfolgung und Gefahrenabwehr. Robert Malte Ruhland behandelt das Thema Mitbestimmungsrechte und überträgt die rechtliche Bewertung auf Big Data-Anwendungen.

Viel Spaß bei der Lektüre wünscht Ihnen
Jaqueline Rüdiger.

Autorinnen und Autoren dieser Ausgabe:

Moritz Eggert
Moritz Eggert, zeitgenössischer Komponist, zeichnet sich als vielseitiger und innovativer Künstler aus, der sich für ein Umdenken im Zugang und Umgang mit zeitgenössischer Musik einsetzt. Er hat bisher mehr als 230 – oftmals genreübergreifende – Werke komponiert. Des Weiteren ist er Autor des „Bad Blog of Musick“, dem meistgelesenen deutschen Blog über zeitgenössische Musik.
Erreichbar über: carolin@wildkatpr.com

Dr. Denis Giffeler
Informatiker, beschäftigt sich seit über 20 Jahren mit Fragestellungen zum elektronischen Publizieren im Internet.
denis@eves-sport.org

Barbara Körffer
Mitarbeiterin des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein. Der Beitrag gibt ausschließlich die persönliche Auffassung der Autorin wieder.
barbara@koerffer.de

Jonas Plass
Medienmanager, aktiver Leistungssportler und Teilnehmer an den Olympischen Spielen in London, muss sich als Betroffener seit 2006 mit ADAMS auseinandersetzen.
jonas@eves-sport.org

Robert Malte Ruhland
Rechtsanwalt, Sachverständiger für Datenschutz, Compliance-Beauftragter und externer Datenschutzbeauftragter in Dortmund. Rechtsanwaltskanzlei Ruhland, Dortmund
info@kanzlei-ruhland.de

Hans-Hermann Schild
Vorsitzender Richter am Verwaltungsgericht Wiesbaden, befasst sich seit fast dreißig Jahren vielseitig mit Themen aus dem Bereich des Rechts auf informationelle Selbstbestimmung und des Datenschutzrechts.
Erreichbar über die DVD-Geschäftsstelle.

Dr. iur. Arnold von Bosse
Rechtsanwalt, Anwaltskanzlei Westphal, Stralsund
info@anwaltskanzlei-westphal.de

Peter Welchering
Journalist für Radio, Fernsehen und Print; publiziert und referiert u. a. zu Datenschutzthemen
peter@welchering.de

Peter Welchering

Vom überwachten Bürger zum gläsernen Menschen – Big-Data-Analysen führen zu verblüffenden und teilweise gefährlichen Ergebnissen

Daten gelten als „Öl des 21. Jahrhunderts“. Und tatsächlich liefern Prognoseverfahren auf der Grundlage von Big-Data-Algorithmen erstaunlich präzise Voraussagen. Doch die hier eingesetzten Wahrscheinlichkeitsberechnungen haben so ihre Tücken.

Eine deutsche Supermarktkette hat durch den Einsatz von Big-Data-Methoden im Jahr 2012 immerhin knapp 90 Megatonnen leicht verderbliches Obst, Gemüse und Frischfleisch weniger entsorgen müssen. Banken nutzen Big Data unter anderem aus sozialen Netzwerken, um die Kreditwürdigkeit ihrer Kunden besser einschätzen zu können.

Versicherungen finden mit ihrer neuen Analysesoftware auf Massendatenbasis gezielter ihre Kunden. Verhaltensprognosen auf der Grundlage von Big-Data-Methoden lassen sich auf vielen Gebieten anwenden. Modegeschäfte ermitteln damit, welche Stilrichtung sich gut verkauft. Telefongesellschaften finden so heraus, welche ihrer Kunden ihren Mobilfunkvertrag kündigen wollen.

Personalberatungen in den USA suchen mit diesen Auswertungsmethoden geeignete Kandidaten für ganz besondere Expertenjobs mit sehr speziellen Anforderungen. Und Nachrichtendienste nutzen Big Data nicht nur für die Massenüberwachung angeblich im Kampf gegen Terrorismus, sondern berechnen damit auch das Verhalten fremder Regierungen.

So hat die National Security Agency die nächsten Schritte der chinesischen Regierung in der Auseinandersetzung mit Japan um die Senkaku-Inseln im ostchinesischen Meer mit einem Simulationsprogramm auf Big-Data-Basis ziemlich präzise prognostiziert. Die NSA-Wissenschaftler werteten dafür nicht nur sämtliche politischen Beiträge in chinesischen Medien über einen Zeitraum von 16 Wochen aus, sondern auch Kommunikations- und Verbindungsdaten hochrangiger chinesischer Politiker und Militärs. Außerdem griffen sie auf Strategieprofile der chinesischen Marine und Luftwaffe zurück, die bei vergleichbaren Vorfällen über einen Zeitraum von 25 Jahren angelegt worden waren.

Die eingesetzten Algorithmen unterliegen zwar der Geheimhaltung. Allerdings haben für die NSA tätige Mathematiker ein entsprechendes Analysesystem auf einer Big-Data-Konferenz im kalifornischen Menlo Park im Herbst 2011 vorgestellt.

Big Data dominiert die Politikberatung in den USA

Das gesamte System besteht aus Software zur Berechnung statistischer Wahrscheinlichkeiten und zur Simulation von Entscheidungen. Erfolgskritisch sind die festgestellten signifikanten statistischen Korrelationen, zum Beispiel zwischen einer martialischen Sprache in den Regierungsverlautbarungen und fehlender Risikobereitschaft bei Militäreinsätzen oder zwischen einem bestimmten Kommunikationsverhalten und politischen Entscheidungen.

Die NSA-Forscher haben im Falle der chinesischen Militärpolitiker etwa herausgefunden, dass die Bereitschaft, einen bewaffneten Konflikt führen zu wollen, sich von unterschiedlichen Kommunikationsprofilen ableiten lässt. Allein welche Angehörigen welcher Interessengruppen im Zentralkomitee der Kommunistischen Partei Chinas in welcher Intensität mit Mitgliedern der eigenen Gruppe oder mit Angehörigen anderer fraktioneller Gruppierungen telefonieren oder mailen, lässt Schlüsse auf die Risikobereitschaft für einen bewaffneten Konflikt zu.

Dabei werden sogenannte Inferenzen, also Abhängigkeiten auf der Grundlage statistischer Wahrscheinlichkeitsberechnungen, ermittelt. Dafür nutzten die NSA-Statistiker für ihre Versuche im Jahr 2011 einen Höchstleistungsrechner, der 16 Billiarden Gleitkommaoperationen pro Sekunde schafft und ein System von 18 Millionen linearer Gleichungen für das Risikoprofil eines Politikers und dessen Verhaltensprognose berechnet.

Aus Wahrscheinlichkeiten werden Ursachen

Allerdings sind diese Prognose-Instrumente ein wenig in Verruf gekommen, weil Geheimdienste damit flächendeckend Menschen überwachen. Für die Wirtschaft ist das gefährlich. Sie braucht diese Instrumente und geht deshalb mit Informationsveranstaltungen und Diskussion über Big Data in die Offensive. „Wir müssen dringend darüber diskutieren, wie wir solche Big-Data-Anwendungen im Marketing, bei den Human Resources und generell in der Unternehmensplanung so gestalten, dass sie tatsächlich konstruktiv sind und nicht destruktiv werden“, fordert Thomas Mosch vom IT-Branchenverband BITKOM.

Die NSA-Affäre hat hier ihre deutlichen Spuren hinterlassen. Immer mehr Anwender und Bürger stehen Big-Data-Anwendungen kritisch gegenüber, weil Geheimdienste sie für flächendeckende Überwachung nutzen. Und sie fragen sich zunehmend: Wie stark spionieren dann auch Unternehmen den Bürger aus, wenn sie Big Data für die Marktforschung oder im Bereich Human Resource einsetzen?

„Eines ist vollkommen unstrittig“, meint Professor Felix Wortmann von der Universität St. Gallen und fährt fort:

„Big Data erschließt ganz neue und bisher nicht gekannte detaillierte Auswertungs- und Prognosemethoden“.

Big-Data-Analysen werden immer dann angewandt, wenn exakt prognostiziert werden soll, was Menschen mit welcher Wahrscheinlichkeit tun. Dafür müssen sehr große Datenmengen erhoben und abgeglichen werden, um die wichtigen Verhaltensmuster zu finden und auf einzelne Fälle und Fragestellungen oder bestimmte Gruppen von Menschen anwenden zu können.

Big Data ist schon ziemlich alt

Die Methode selbst ist schon recht alt. So haben die Vertriebsspezialisten der amerikanischen Supermarktkette Wal-Mart Ende der 1980er Jahre herausgefunden, dass junge Männer, die abends Babywindeln einkaufen, auch einen Sixpack Bier in den Einkaufswagen legen. Diese statistisch signifikante Korrelation haben sie bei einer Auswertung von Kassenzetteln und Kreditkartendaten entdeckt.

Als Konsequenz wurden Sixpacks und Windeln nebeneinander in die Regale gestellt, um den Einkaufkomfort für die gestressten jungen Väter zu erhöhen. Die dankten das nicht nur durch besondere Kundentreue, sondern auch, indem sie den einen oder anderen Knabberartikel zusätzlich kauften, der in unmittelbar räumlicher Nähe von Sixpacks und Windeln angeboten wurde.

Wal-Mart entwickelte daraus ein Programm für die Sortimentspräsentation, mit dem besonders hohe Abverkaufszahlen erzielt wurden. Die Zahl der Parameter zur Ermittlung der statistisch signifikanten Korrelationen war recht überschaubar und ließ sich auch mit leistungsschwachen Buchhaltungscomputern nebenher berechnen.

Wesentlich mehr rechnerischen Aufwand musste da schon die Chase Manhattan Bank treiben, als sie ebenfalls Ende der 1980er Jahre ein Prognosesystem entwickelte, um die Insolvenzwahrscheinlichkeit ihrer Kunden besser abschätzen zu können. Hierfür wurden die auffälligsten Korrelationen zwischen dem Kauf- und Bezahlungsverhalten der Kunden und den tatsächlich eingetretenen Insolvenzen pro Geschäftsjahr ermittelt.

Im Mittelpunkt steht die Verhaltensprognose

Dabei ergab sich, dass Kunden, die häufiger mit ihrer Kreditkarte Einkäufe bezahlten, ihre Barabhebungen am Bankschalter drastisch reduzierten und von teurer Qualitätsware vor allen Dingen bei Bekleidung auf Billig- und Sonderangebote umstiegen, extrem häufig zahlungsunfähig wurden. Die Bankmanager ließen eine Software für die Mustererkennung programmieren, die wöchentlich das Kauf- und Zahlungsverhalten der Kunden auswertete und daraus einen sogenannten Insolvenzkoeffizienten errechnete. Kunden mit erhöhter Insolvenzwahrscheinlichkeit wurden dann aktiv von ihrem Bankberater angesprochen.

Nach derselben Methode, aber auf einer wesentlich größeren Datenbasis arbeitet gegenwärtig ein System für bessere Kundenbindung, das der Mobilfunkanbieter Vodafone betreibt. Damit werden die am stärksten wechselwilligen Kunden identifiziert, denen dann bestimmte Bonusprogramme, Freiminuten oder neue Handymodelle angeboten werden, wenn sie ihren Vertrag verlängern.

„Grundlage solcher Kundenbindungsprogramme sind zumeist Kommunikationsdaten“, meint Professor Michael Feindt, dessen Blue Yonder GmbH wohl die derzeit leistungsstärksten Analysepakete für Big-Data-Auswertungen am Markt hat. „Die statistisch signifikanten Korrelationen werden in einem mehrdimensionalen Analyseverfahren ermittelt“, erläutert Professor Feindt, der seine ersten Big-Data-Analyseprogramme am europäischen Kernforschungszentrum CERN in Genf entwickelt hat.

Die Prognosegüte der Sicherheitsbehörden ist miserabel

Die Prognosegüte hängt dabei auch wesentlich von der Fehlerberechnung und Plausibilitätsanalyse ab. „Die bloße Wahrscheinlichkeitsberechnung nur der Kriterien zur Ermittlung einer Korrelation reicht nicht“, urteilt Big-Data-Spezialist Michael Feindt. Die dafür massenhaft erhobenen und ausgewerteten Daten müssen zuvor um einzelne Ausreißer bereinigt werden. Und jede gefundene Abhängigkeit oder Inferenz wird noch einmal auf verschiedene Fehlerfaktoren hin analysiert.

Auch erste Versicherungen arbeiten bereits mit derartigen Analysemethoden. Allerdings sind die in der Regel nicht von externen Dienstleistern zugekauft, sondern von den Versicherungsmathematikern im eigenen Haus entwickelt.

Damit konnte eine Versicherungsgesellschaft die Abschlussquote für Ausbildungsversicherungen von einem einstelligen Wert bei traditionellen Massenmailings auf deutlich über 90 Prozent bei Big-Data-gestützten Verfahren erhöhen. Dabei wertet nur für diesen Zweck entwickelte Suchsoftware soziale Netzwerke nach Mitteilungen über Neugeborene aus. Eine Identifikationssoftware ermittelt die frischgebackenen Eltern, per Geolokalisation wird vollautomatisch überprüft, ob der Wohnort in einem Gebiet mit ausreichendem Kaufkraftindex liegt.

Zusätzlich wertet eine Mustererkennungssoftware aus, ob die identifizierten Eltern aufgrund ihres Kommunikationsverhaltens eher sicherheitsaffin oder risikoaffin sind. Den sicherheitsaffinen Eltern wird dann ein individuelles Angebot einer Ausbildungsversicherung fürs Kind unterbreitet.

Im Kreditgeschäft ist Big Data gefährlich

Die Kombination von Verknüpfungsalgorithmen zur Erkennung von statistisch signifikanten Korrelationen mit Mustererkennungssoftware zum Abgleich mit Verhaltensprofilen wird auch von Sicherheitsbehörden in der Kriminalprävention eingesetzt. Die von der Europäischen Kommission geförderten Indect-Forschungsprojekte sind neben den amerikanischen Präventionsprojekten am weitesten fortgeschritten.

Dort wird zum Beispiel das Verhalten von Reisenden an Bahnhöfen per Kamera überwacht. Eine Software für die Verhaltensprognose schlägt dann Alarm, wenn sich ein Reisender verdächtig verhält. „Der springende Punkt ist, wie dann das sogenannte verdächtige Verhalten definiert wird“, gibt der Berliner Computerexperte Benjamin Kees zu bedenken.

Reicht es schon aus, wenn ein einzelner Reisender sich in seinem Verhalten vom Normverhalten der Mehrheit unterscheidet, also zum Beispiel einen etwas anderen Weg zum Bahnsteig nimmt als der Durchschnitt oder in seiner Körpersprache von einer Norm abweicht?

Metadatenanalyse sind klassische Big-Data-Anwendungen

Solche Fragen sind vor allen Dingen im Zusammenhang mit der NSA-Überwachungsaffäre im Sommer 2014 wieder stärker diskutiert worden. Denn die Überwachungsprogramme der NSA werten zum Beispiel die Metadaten zum Kommunikationsverhalten der Menschen aus.

Verbindungsdaten, genutzte Kommunikationsmedien in ihrer Abfolge und Zeitstempel für die Verbindungen sowie Aufenthaltsorte sind in der Vergangenheit automatisiert so überwacht worden. Alarm wurde dann ausgelöst, wenn das Kommunikationsverhalten dem Verhaltensprofil entsprach, das die Auswerter in der Vergangenheit bei Terroristen festgestellt hatten. Dann wurde der einzelne Mensch direkt überwacht, wurden seine Mails mitgelesen oder Gesprächsinhalte ausgewertet, sein Computer mittels Online-Durchsuchung ausgeforscht.

Doch die ermittelten Verhaltensmuster mit ihren Verknüpfungen waren nicht fein genug. Deshalb haben die Überwachungscomputer zu oft Alarm ausgelöst. Das verursacht Kosten und wurde auch zum politischen Problem. Deshalb wollen die NSA-Analysten auch hier Verhaltensprognosen per Simulation erstellen lassen. Doch was zur Ermittlung des wahrscheinlichen Verhaltens einer Regierung wie im Falle der Auseinandersetzung um die Senkaku-Inseln noch machbar war, erweist sich bei einer massenhaften Überwachung zumindest mit den bisherigen Rechenkapazitäten als nicht realisierbar.

Immerhin musste für die Verhaltensprognose eines Politikers ein System von mindestens 18 Millionen Gleichungen berechnet werden. Damit sind herkömmliche Supercomputer einige Tage beschäftigt. Reduziert man jedoch die Berechnungspunkte für das Verhalten und kommt so auf ein System von zwei bis drei Millionen linearer Gleichungen, wird die Verhaltensprognose zu ungenau.

Deshalb setzen die NSA-Analysten auf die Entwicklung neuer Supercomputer, die zehntausendmal schneller rechnen als die bisher entwickelten. In der Zwischenzeit geben sie sich mit einer geringeren Trefferquote bei der Verhaltensprognose zufrieden und investieren lieber in personalintensive Direktüberwachung oder setzen auf vorsorgliche Verhaftung oder Ausweisung, je nach Rechtsstatus.

„Dabei wird bewusst davon abgelenkt, dass wir es hier nicht mit Fakten zu tun haben, sondern nur mit der Berechnung von bloßen Wahrscheinlichkeiten“, warnt Professor Günter Müller von der Universität Freiburg vor der Big-Data-Gläubigkeit der Sicherheitsbehörden.

Barbara Körffer

Auswertung personenbezogener Daten für Strafverfolgung und Gefahrenabwehr – genügen die gesetzlichen Grundlagen zum Schutz des Rechts auf informationelle Selbstbestimmung?

I. Einführung

Die Auswertung von Daten, um Schwerpunkte und Entwicklung von Kriminalität und von Gefahren für die öffentliche Sicherheit zu erkennen und daraus Einsatzschwerpunkte für die polizeiliche Arbeit abzuleiten, sowie die operative Auswertung von Informationen aus Strafverfahren, um Zusammenhänge zwischen Taten und Tätern zu erkennen und damit Serienstraftaten sowie organisierte Kriminalität aufzuklären, ist seit jeher Bestandteil polizeilicher und kriminalistischer Arbeit. Schritt für Schritt sind diese Prozesse in den vergangenen Jahren automatisiert worden. Zur Unterstützung der Auswertung werden vielerlei automatisierte Verfahren eingesetzt, die etwa die Verbindungen zwischen Tätern, Tatbeteiligten, Tatausführungen und Objekten herstellen und visualisieren. Die fortschreitende Verbreitung von Big-Data-Technologien lässt erahnen, dass die Entwicklung computergestützter Auswertungs- und Ermittlungsarbeit noch lange nicht ihr Ende erreicht hat. Deutsche Polizeibehörden testen bereits Produkte für die Vorhersage künftiger Ereignisse, so genanntes predictive policing. Solche Vorhersagen können auf allgemeine, nicht personenbezogene, Entwicklungen ausgerichtet sein, sind aber zumindest in künftigen Entwicklungsstufen auch als personenbezogen denkbar. Forschungsvorhaben beschäftigen sich mit Möglichkeiten der Analyse großer und vielfältiger Datenmengen, u.a. aus sozialen Netzwerken, mit Data Mining zur Aufklärung von Kriminalität.

Mit der steigenden Automatisierung nehmen auch die Risiken für das Recht auf informationelle Selbstbestimmung

der Betroffenen zu. Dies beginnt bei den Rohdaten, die als Grundlage für die Auswertungen verwendet werden. Mit steigender Menge und Vielfalt steigt das Risiko für Unbeteiligte, in solche Auswertungen einbezogen zu werden. Dies gilt insbesondere dann, wenn unstrukturierte Daten ausgewertet werden, da sie häufig nicht nur Informationen über Tatverdächtige, sondern auch über Dritte enthalten. Fortgesetzt wird die Gefährdung durch Auswertemethoden, die eigenständig nach Mustern und Zusammenhängen suchen. Dies wirft nicht nur Fragen hinsichtlich der Transparenz auf, sondern erhöht die Gefahren für Unbeteiligte, durch zufällige Übereinstimmung ihrer Verhaltensmuster mit den von den Algorithmen als signifikant erkannten Mustern als auffällig erkannt zu werden. Angesichts dieser Risiken und der Verbreitung, die solche Systeme zunehmend finden, ist es an der Zeit zu fragen, ob und inwieweit das geltende Recht ausreichende Schutzmechanismen bietet.

II. Gesetzliche Befugnisse zur Auswertung personenbezogener Daten

Den Kern von Big-Data-Anwendungen bilden Werkzeuge zur Auswertung der Daten. Dabei sind für polizeiliche Zwecke unterschiedliche Auswertungen vorstellbar. Ganz ohne Personenbezug sind strategische Auswertungen denkbar, die auf der Grundlage der polizeilichen Daten und ggf. auch weiterer nicht personenbezogener Daten abstrakte Lagebilder erstellen, etwa zur Entwicklung bestimmter Kriminalitätsphänomene oder zur Entwicklung von Kriminalitätsräumen in Städten. Solche Anwendungen können auch eingesetzt werden, um ohne Personenbezug künftige Entwicklungen zu prognostizieren. Operative Auswertungen hingegen sind in der Regel auf die Auswertung bestimmter Straftaten, Seriendelikte, Tätergruppen, kriminellen Netzwerke und ähnlich personenbezogene Phänomene gerichtet. Hier wird eine anonyme Auswertung kaum in Betracht kommen. Daher stellt sich gerade für diese Auswertungen die Frage nach der rechtlichen Zulässigkeit, die im Folgenden untersucht werden soll.



Bild: ClipDealer.de

1. Nutzung personenbezogener Daten

Die Auswertung von personenbezogenen Daten ist ein eigenständiger Grundrechtseingriff und bedarf daher einer gesetzlichen Grundlage. Nach den Maßstäben des Bundesdatenschutzgesetzes (BDSG) handelt es sich bei der Auswertung um eine Nutzung personenbezogener Daten im Sinne des § 3 Abs. 5 BDSG. Bemerkenswert ist in diesem Zusammenhang, dass die Nutzung erst bei der Novellierung des Bundesdatenschutzgesetzes im Jahr 1990 als eigenständige Phase der Verwendung personenbezogener Daten in das Bundesdatenschutzgesetz aufgenommen und so dem Gesetzesvorbehalt unterstellt wurde. Besondere Konturen hat diese Phase der Datenverarbeitung seitdem durch den Gesetzgeber allerdings nicht erfahren. Nach wie vor liegt der Schwerpunkt der Datenschutzregulierung, gerade für die Strafverfolgung und die Gefahrenabwehr, in der Phase der Erhebung der Daten. Für die Realität der Datenverarbeitung in den Jahren 1977 und auch 1990 mag diese Schwerpunktsetzung sachgerecht gewesen sein. Begreift man die Nutzung als den bestimmungsgemäßen Gebrauch einzelner Daten, ist ihr Eingriffspotential gering. Die heutige Realität sieht jedoch anders aus und erlaubt technisch bereits jetzt umfangreiche Auswertungen personenbezogener Daten, die sich nicht auf einzelne Daten und nicht auf den Zweck beschränken, für den sie erhoben wurden.

Für Daten aus Strafverfahren erlaubt § 483 StPO die Speicherung und Nutzung in Dateien, soweit dies für Zwecke des Strafverfahrens erforderlich ist. Die Zweckbestimmung bezieht sich hier auf das bestimmte Strafverfahren, für das die Daten erhoben worden sind. Dies ergibt sich eindeutig aus dem Gesetz selbst, denn § 483 Abs. 2 StPO erlaubt ausdrücklich die Nutzung der nach Absatz 1 gespeicherten Daten für andere Strafverfahren. Diese Befugnis wäre überflüssig, wenn der Zweck in Absatz 1 bereits die Strafverfolgung als solche umfassen würde.

2. Abgleich

Werden Daten mit anderen Daten abgeglichen, sind für den Abgleich weitere Vorschriften zu beachten. Die Strafprozessordnung unterscheidet zwei Varianten des Abgleichs: den „einfachen“ Datenabgleich in § 98c StPO und die Rasterfahndung in § 98a StPO. Gleiches gilt für die präventiv-polizeilichen Regelungen in den Polizeigesetzen des Bundes und der Länder. Die Regelungen sind im Jahr 1992 in die Strafprozessordnung aufgenommen worden und seitdem unverändert. Auch die Rechtsprechung hat diese Regelungen – mit Ausnahme der Einschränkungen der Rasterfahndung im präventiv-polizeilichen Bereich durch das Bundesverfassungsgericht – nicht weiter ausgeprägt.

a) Die Rasterfahndung

§ 98a StPO erlaubt einen maschinellen Abgleich von Daten aus mehreren unterschiedlichen Quellen, die nicht von der Polizei stammen, sondern bei anderen öffentlichen oder von nicht öffentlichen Stellen eigens für die Rasterfahndung

erhoben werden. Ziel der Maßnahme ist der Ausschluss von Nichtverdächtigen oder die Feststellung von Personen, die weitere für die Ermittlungen bedeutsame Prüfungsmerkmale erfüllen. Kennzeichnend für diese Maßnahme ist ihre Streubreite. Naturgemäß wird eine Vielzahl eigentlich unbeteiligter Personen in die Rasterung einbezogen. Gegen keine dieser Personen besteht ein Tatverdacht, sondern erst durch die Rasterung sollen überhaupt Verdächtige gefunden werden, gegen die im Anschluss Ermittlungen geführt werden können. Grundrechtseingriffe, die sowohl durch Verdachtslosigkeit als auch durch eine große Streubreite gekennzeichnet sind – bei denen also zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben – weisen grundsätzlich eine hohe Eingriffsintensität auf. Sie beeinträchtigen nicht nur den Einzelnen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens ist. Solche Eingriffe bedürfen einer näheren Eingrenzung, damit sie als verhältnismäßig angesehen werden können. Diese Eingrenzung nimmt der Gesetzgeber für das Strafverfahren dadurch vor, dass zureichende tatsächliche Anhaltspunkte für eine Straftat von erheblicher Bedeutung nach einem abschließend aufgeführten Katalog vorliegen müssen. Im präventiv-polizeilichen Bereich darf die Rasterfahndung nur bei Vorliegen einer konkreten Gefahr durchgeführt werden. Hinzu kommen Verfahrenssicherungen wie die Anordnung durch ein Gericht, die Pflicht zur unverzüglichen Löschung der übermittelten Daten nach Beendigung des Abgleichs sowie die Pflicht zur Unterrichtung der zuständigen Datenschutzbehörde und zur Benachrichtigung der Betroffenen nach § 101 StPO.

Die Datenauswertung bei der Rasterfahndung ist zwar nicht hinsichtlich der Quellen und der Menge der einbezogenen Personen, dafür aber nach der Art der für die Rasterung zu verwendenden Daten begrenzt. In einer ersten Stufe fordert die Polizei- bzw. Strafverfolgungsbehörde von bestimmten Behörden oder Unternehmen abschließend festgelegte Daten über Personen (in der Regel Identifizierungsmerkmale wie Name, Anschrift, Geburtsdatum, Geburtsort) an, die bestimmte – ebenfalls zuvor festgelegte – Merkmale erfüllen. Die von den externen Stellen übermittelten Daten werden von der Polizei bzw. Strafverfolgungsbehörde in einer zweiten Stufe miteinander und mit polizeilichen Dateien abgeglichen. Gegen die daraus entstandene Schnittmenge von Personen werden im Anschluss bei hinreichenden Anhaltspunkten mit regulären Ermittlungsmethoden weitere Ermittlungen geführt.

Somit erlaubt § 98a StPO die eigentliche polizeiliche Auswertung nur in begrenztem Umfang. Für die Auswertung werden nur Daten genutzt, die zuvor abschließend festgelegte Kriterien erfüllen. In der Regel enthält der so von den übermittelnden Stellen selektierte Datenbestand strukturierte Datensätze mit wenigen Merkmalen.

Der eingangs skizzierte Funktionsumfang von Big-Data-Auswertungen wird durch diese Regelung bei weitem nicht abgedeckt. § 98a StPO ist daher keine Rechtsgrundlage für offen gestaltete Auswertungen auf einer breiten, nicht nach Selektionskriterien eingegrenzten, Datenbasis.

b) Der maschinelle Datenabgleich

aa) Rechtsgrundlagen

Der maschinelle Abgleich personenbezogener Daten aus Strafverfahren ist nach §98c StPO und für Daten aus Gefahrenabwehrvorgängen nach den Polizeigesetzen der Länder erlaubt. Die Regelungen entsprechen einander in ihren Voraussetzungen weitgehend. So ermächtigt § 98c StPO die Strafverfolgungsbehörden, zur Aufklärung einer Straftat personenbezogene Daten aus Strafverfahren mit anderen zur Strafverfolgung oder Strafvollstreckung oder zur Gefahrenabwehr gespeicherten Daten maschinell abzugleichen. Die Vorschrift ist materiell weitgehend und formell vollständig voraussetzungslos. Damit ermächtigt sie nur zu geringfügigen Grundrechtseingriffen. Der Abgleich steht einzig unter dem allgemeinen Vorbehalt des Verhältnismäßigkeitsgrundsatzes, d.h. er muss für den in der Norm angegebenen Zweck der Strafverfolgung geeignet, erforderlich und angemessen sein. Eine weitere Einschränkung erhält die Befugnis durch die Benennung der Daten, die für den Abgleich genutzt werden dürfen. Durch die Beschränkung auf „Daten aus einem Strafverfahren" und „zur Strafverfolgung, Strafvollstreckung oder Gefahrenabwehr gespeicherten Daten" wird klargestellt, dass nur Daten abgeglichen werden dürfen, die die Strafverfolgungsbehörden bzw. die Polizei bereits im Rahmen ihrer Aufgaben erhoben hat. Nach überwiegender Auffassung in der strafrechtlichen Literatur folgt daraus bereits die Beschränkung auf lediglich unbedenkliche Grundrechtseingriffe. Dies wird damit begründet, dass „die Strafverfolgungsbehörden beim Datenabgleich lediglich bereits bei ihnen bevorratetes Wissen nutzen." Diese Differenzierung ist wenig nachvollziehbar und reicht allein nicht aus, um eine verhältnismäßige Anwendung des § 98c StPO sicherzustellen. Denn der Umstand, ob die Daten bereits bei der Polizei vorhanden sind oder eigens für eine Auswertung bei anderen Stellen erhoben werden müssten, bedeutet im Ergebnis keinen gravierenden Unterschied. Dabei ist erstens zu berücksichtigen, dass letztlich nahezu alle Erkenntnisse, die die Polizei zur Strafverfolgung oder Gefahrenabwehr ermittelt, aus externen Quellen stammen, seien es als Beweismittel beschlagnahmte Daten, Berichte von Zeugen, Daten aus dem Melderegister, Telekommunikationsverkehrsdaten, Daten über Bankkonten oder andere Informationen. Zweitens ist zu berücksichtigen, dass solcherlei Informationen für laufende Strafverfahren bereits in großen Mengen bei der Polizei vorhanden sind. Schließlich ist drittens zu beachten, dass solche Daten – auch wenn sie bereits für ein Strafverfahren erhoben wurden – bei weitem nicht nur Daten über Tatverdächtige und unmittelbar ermittlungsrelevante Informationen enthalten. Vielmehr sind gerade in unstrukturierten Daten, aber auch in strukturierten Daten wie beispielsweise den Ergebnissen einer nicht individualisierten Funkzellenabfrage, häufig Informationen über Dritte enthalten, die an der Straftat vollkommen unbeteiligt

sind und nur durch Zufall von den Ermittlungen erfasst wurden. Würde man eine Auswertung uneingeschränkt unter den Voraussetzungen des § 98c StPO zulassen, würde dies bedeuten, dass sämtliche bei Polizeibehörden vorhandenen Daten auf der Grundlage eines Anfangsverdachts für eine Straftat gegeneinander abgeglichen werden könnten. Dies überstiege den Rahmen des § 98a StPO für die Rasterfahndung bei weitem.

Dies war offensichtlich bei Einführung der Vorschrift im Jahr 1992 nicht beabsichtigt, wenngleich dies weder im Gesetz noch in Begründung zum Ausdruck gekommen ist, sondern lediglich bei Hilger in einer Fußnote klargestellt wird: „§§ 98c darf nicht zu einer Umgehung der speziellen, einschränkenden Voraussetzungen der §§ 98a, 98b herangezogen werden: Ist in einem Strafverfahren z.B. eine Datei als Beweismittel beschlagnahmt und enthält sie Daten, die für ein anderes Verfahren Ausgangspunkt einer Rasterfahndung sein könnten, so sind insoweit §§ 98a, 98b zu beachten."

bb) Einschränkende Auslegung

Somit bedarf die Vorschrift zumindest einer eingeschränkten Auslegung, damit sie in verfassungskonformer Weise angewandt wird und nicht zu einer Befugnis für eine polizei-interne „Rasterfahndung" erwächst. Eine sinnvolle Einschränkung kann erreicht werden, wenn man den Begriff der „personenbezogenen Daten aus einem Strafverfahren" in § 98c StPO in Abgrenzung zu § 98a StPO begrenzt auf Daten zu Personen, gegen die bereits ein Anfangsverdacht vorliegt. Dadurch wird die Auswertung von vornherein auf Tatverdächtige konzentriert und eine Auswertung zur Verdächtigengewinnung – die ja Wesensmerkmal der Rasterfahndung ist – wäre ausgeschlossen. Eine weitere Eingrenzung kann durch Auslegung des Begriffs der „anderen zur Strafverfolgung oder Strafvollstreckung oder zur Gefahrenabwehr gespeicherten Daten", der Referenzdaten, erreicht werden. Werden diese Daten für einen Abgleich genutzt, handelt es sich hinsichtlich dieser Daten um eine Zweckänderung. Denn in der Regel werden die Referenzdaten nicht mehr für das konkrete Verfahren verwendet, für das sie erhoben wurden, sondern für ein neues Verfahren. Eine solche Zweckänderung bedarf einer gesetzlichen Befugnis, und es ist fraglich, ob § 98c StPO bereits als ausreichend bestimmte Rechtsgrundlage für die Zweckänderung angesehen werden kann. Näher liegt die Annahme, dass nur solche Daten für den Abgleich verwendet werden sollen, die bereits für andere als die ursprünglichen Zwecke in Dateien gespeichert werden, also etwa Dateien nach § 484 StPO oder die präventiv-polizeilichen INPOL-Dateien wie z.B. Fahndungsdateien, Erkennungsdienstdatei oder Kriminalaktennachweis. Die Speicherung in solchen Dateien setzt stets eine Prüfung der Relevanz für die jeweiligen Zwecke der Datei voraus. Als Beispiel hierfür sei § 8 BKAG für die beim Bundeskriminalamt geführten Dateien genannt. Danach dürfen in erster Linie Daten von Beschuldigten und Verdächtigen gespeichert werden; für die Speicherung von Daten, die über den Katalog der Grunddaten des § 8 Abs. 1 BKAG hinausgehen, ist eine Prognose zu treffen, ob Grund zu der Annahme besteht, dass der Betroffene (erneut) Straftaten begehen wird. Diese Dateien unterliegen ihrerseits wiederum einer Zweckbestimmung, die in den jeweiligen Errichtungsanordnungen nach § 490 StPO, § 34 BKAG oder den Polizeigesetzen der Länder festgelegt ist. Diese Zweckbestimmung ist beim Abgleich zu berücksichtigen, d.h. ein Abgleich mit Dateien darf nur im Rahmen der Zweckbestimmung dieser Dateien vorgenommen werden.

Schließlich stellt sich die Frage, welche Art von Auswertungen der Begriff des maschinellen Abgleichs in § 98c StPO erlaubt. Zwischen einer einfachen Suchanfrage nach dem Namen einer Person in einer Datenbank und einer komplexen Auswertung, die eventuell auch selbstlernend nach übereinstimmenden Mustern sucht, bestehen im Hinblick auf die Grundrechtsgefährdung erhebliche Unterschiede. So hat das Bundesverfassungsgericht die ebenfalls ohne qualifizierte Eingriffsschwellen ausgestaltete Nutzungsregelung des § 5 ATDG für die in der Antiterrordatei gespeicherten Daten nur deshalb als verfassungskonform angesehen, weil diese Vorschrift „lediglich Einzelabfragen, nicht aber auch eine Rasterung, Sammelabfragen oder die übergreifende Ermittlung von Zusammenhängen zwischen Personen durch Verknüpfung von Datenfeldern erlaubt. Die Vorschrift setze damit einen konkreten Ermittlungsanlass voraus. Auch stehe jede Abfrage unter der im Einzelfall sachhaltig zu prüfenden Voraussetzung der Erforderlichkeit. Im Übrigen ermächtige sie nach ihrer derzeitigen Ausgestaltung weder zu einer automatischen Bilderkennung noch zur Verwendung von Ähnlichenfunktionen oder zur Abfrage mit unvollständigen Daten (so genannten „wildcards"). Ob diese Grundsätze auf den Datenabgleich nach § 98c StPO und den präventiv-polizeilichen nach den Polizeigesetzen vollständig übertragbar ist, ist fraglich. Dagegen spricht, dass die Datei aufgrund der gemeinsamen Nutzung durch Polizeibehörden und Nachrichtendienste eine besondere Eingriffsintensität aufweist und dass außerdem jede einzelne Speicherung in der Antiterrordatei aufgrund der damit für den Betroffenen verbundenen negativen Konsequenzen stets mit einem erheblichen Grundrechtseingriff verbunden ist, der die Intensität der Speicherung in anderen polizeilichen Dateien übertreffen kann. Dafür spricht jedoch, dass die Antiterrordatei im Vergleich zu anderen polizeilichen Dateien einen nur geringen Teil der Bevölkerung abbildet und das Gesetz vergleichsweise hohe Schwellen für die Speicherung vorsieht. Auch ein Vergleich mit Abgleichsvorschriften in anderen Gesetzen, wie etwa dem Melderecht, verdeutlicht, dass der Gesetzgeber in anderen Fällen die Modalitäten eines automatisierten Abgleichs bzw. Abrufs durchaus präzise regelt. Somit spricht Vieles dafür, dass § 98c StPO nur einfache Datenbankabfragen, nicht aber komplexere Recherchen und Auswertungen erlaubt.

Verfassungsrechtlich besonders problematisch sind Auswertungen mit den Methoden des Data Mining, die häufig Bestandteil moderner Big-Data-Anwendungen sind. Selbstlernende Algorithmen werten Daten nach bislang unbekannten Mustern aus und finden Zusammenhänge auf der Grundlage der von ihnen erkannten Kriterien und Muster. Bei solchen Auswertungsverfahren ist nur schwer vorstellbar, wie bereits vor Verwendung der Daten die

Erforderlichkeit einer Suche festgestellt werden kann, wie es der Grundsatz der Erforderlichkeit verlangt. Auch an die Transparenz stellen diese Auswertungsmethoden hohe Anforderungen, da es zumindest im Nachhinein möglich sein muss, das Zustandekommen des Ergebnisses vollständig nachvollziehen zu können. Damit sind nur zwei der vielen Fragen angesprochen, die Big-Data-Anwendungen aufwerfen, doch sie verdeutlichen bereits, dass angesichts der damit verbundenen Herausforderungen für die Gewährleistung des Rechts auf informationelle Selbstbestimmung eine schlichte Befugnisnorm wie § 98c StPO nicht ausreichen kann, um solche Anwendungen zu erlauben.

3. Nutzung von Daten aus öffentlich zugänglichen Quellen

Dieselben Grundsätze gelten, soweit personenbezogene Daten aus allgemein zugänglichen Quellen genutzt werden. Von praktischer Bedeutung ist dies vor allem für die im Internet veröffentlichten Daten. Diese Daten fallen unter den Schutz der Datenschutzgesetze und unterliegen ebenfalls einer Zweckbindung, wie § 14 Abs. 2 Nr. 5 BDSG klarstellt. Die bloße Kenntnisnahme von Informationen, die z.B. im Internet veröffentlicht sind, mag die Schwelle zum Grundrechtseingriff noch nicht erreichen. Werden personenbezogene Daten aus allgemein zugänglichen Quellen aber gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet und ergibt sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen, liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung vor. Die gezielte Speicherung von personenbezogenen Daten aus dem Internet ist damit als Grundrechtseingriff anzusehen, für die Auswertung solcher Daten und den Abgleich mit anderen Daten und Dateien gilt dies ebenfalls. Eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen, die nach der Entscheidung des Bundesverfassungsgerichts für den Grundrechtseingriff ebenfalls ausschlaggebend sein soll, ist bei Informationen aus dem Internet schnell erreicht. Bereits die allgemein zugänglichen Informationen aus dem Internet sind häufig so vielfältig, dass aus ihnen schon aussagekräftige Profile über Personen erstellt werden können. Durch Verknüpfung mit anderen Daten können diese Profile weiter angereichert werden, was die Gefahrenlage nochmals erhöht. Für den Abgleich personenbezogener Daten aus dem Internet mit polizeilichen Daten bedarf es daher einer Rechtsgrundlage. § 98c StPO kommt hier in Betracht, es sind aber dieselben Einschränkungen zu beachten wie beim Abgleich anderer im Strafverfahren gewonnenen Daten. Dies verbietet einen anlasslosen Abgleich von allgemein zugänglichen Daten und den Abgleich von Daten solcher Personen, die nicht als Verursacher einer Straftat oder Gefahr in Betracht kommen.

4. Transparenz der Auswertung

Die Transparenz der Datenverarbeitung für die Betroffenen ist eine der wesentlichen Voraussetzungen dafür, dass informationelle Selbstbestimmung gewährleistet werden kann. Doch nicht nur für die Betroffenen ist Transparenz von Bedeutung, sondern zunächst vor allem für die verantwortliche Stelle selbst. Da das Datenschutzrecht negative Entscheidungen für Betroffene, die ausschließlich auf einer automatisierten Verarbeitung von Persönlichkeitsmerkmalen beruhen, verbietet (§ 6a BDSG), kann das Ergebnis einer automatisierten Auswertung stets nur vorbereitend oder unterstützend für die endgültige Entscheidung durch den Sachbearbeiter herangezogen werden. Dafür muss es vollständig transparent und nachvollziehbar sein. Auch dem Betroffenen muss das Ergebnis der automatisierten Auswertung und sein Zustandekommen offen gelegt werden, damit sich er nach den Grundsätzen des rechtsstaatlichen Verfahrens dagegen verteidigen kann.

III. Ergebnis und Ausblick

Die Strafprozessordnung und die Polizeigesetze erlauben Auswertungen nur in einem engen Rahmen. Externe Daten dürfen nur stark eingeschränkt ausgewertet werden. Nach Maßgabe der Vorschriften über die Rasterfahndung dürfen externe Daten ausgewertet werden, die nach festgelegten Kriterien von festgelegten Stellen vorselektiert wurden. Nach den Vorschriften über den maschinellen Datenabgleich dürfen nur Daten ausgewertet werden, die bereits für ein Strafverfahren erhoben wurden und Tatverdächtige betreffen. Komplexe Analysen großer und vielfältiger Datenmengen mit Data-Mining-Methoden können darauf nicht gestützt werden. Es drängt sich bereits die Frage auf, ob sie für alle gegenwärtigen Formen der polizeilichen Datenauswertungen ausreichend sind. Soll die Zukunft der Polizeiarbeit in der automatisierten Auswertung von Daten, unterstützt durch intelligente Systeme, liegen, kann und darf diese Entscheidung nicht ohne den Gesetzgeber getroffen werden.

Die geltenden Gesetze, die im Bereich der Datenerhebung in den letzten Jahren ständig aktualisiert und auf jede neue Erhebungsmaßnahme angepasst wurden, sind für die Phase der Nutzung der Daten seit 1992 unverändert geblieben. Für eine weitergehende Automatisierung polizeilicher Arbeit wären klare und begrenzende Eingriffsbefugnisse zu formulieren, damit der Schutz des Rechts auf informationelle Selbstbestimmung auch bei Big-Data-Anwendungen gewährleistet wird. Eine uneingeschränkte Nutzung von Big-Data-Anwendungen wird jedoch auch durch Gesetze nicht zugelassen werden können. Hier gibt es verfassungsrechtliche Grenzen zu beachten, die dem entgegenstehen. Auf Eingriffsschwellen, die einen Anlass für die Maßnahme voraussetzen, kann nicht verzichtet werden. Das Bundesverfassungsgericht hat mehrfach verdeutlicht, dass es keine vollständig anlasslosen Maßnahmen geben darf. So wäre etwa der Einsatz der Befugnisse des Bundesnachrichtendienstes, verdachtslos Fernmeldeverkehre zu überwachen und sie durch Abgleich mit Suchbegriffen auszuwerten, für Zwecke der personenbezogenen Risikoabwehr im Bereich der inneren Sicherheit in jedem Fall unverhältnismäßig und damit verfassungswidrig. Dass die Maßnahme selbst durch einen hinreichenden Anlass gerechtfertigt sein muss, bedingt zwar noch nicht, dass auch die davon betroffenen Personen in einem Zusammenhang zu diesem Anlass stehen müssen. Solche Maßnahmen, die sich gegen eine Vielzahl von Unbeteiligten richten, müssen aber durch Gesetz auf das absolut notwendige Maß beschränkt werden.

Robert Malte Ruhland

Big Data und Mitbestimmung

Der Beitrag stellt eine allgemeine Einführung und eine allgemeine Übersicht über Big-Data-Anwendungen mit personenbezogenen Beschäftigtendaten dar, zeigt die möglichen Rechte der Belegschaftsvertretungen und gibt Hinweise für einen verhältnismäßigen und rechtmäßigen Umgang mit Beschäftigtendaten sowie Beispiele für Big-Data-Anwendungen mit Beschäftigtendaten.



Zurzeit kommen Big-Data-Anwendungen, die auf Beschäftigtendaten basieren, insbesondere in den Bereichen des Recruitings, Talent Managements, der Personalplanung und der Leistungsmessung zum Einsatz.

In einigen Big-Data-Anwendungen werden diese Daten dann zu nicht personenbezogenen Daten in Korrelation gesetzt. Diese Daten können in Big-Data-Anwendungen regelmäßig zur Erfassung des Ist-Zustandes, vor allem aber auch für prognostische Entscheidungen genutzt werden.

Big-Data-Anwendungen können aber darüber hinaus beispielsweise auch genutzt werden um den Wahrheitsgehalt von z. B. verschriftlichten Aussagen zu messen. Dies ist natürlich umso leichter, je mehr Kommunikation des Beschäftigten als Vergleichsmaterial vorhanden ist. Man denke in diesem Zusammenhang beispielsweise an archivierte E-Mails, Einträge in sozialen Netzwerken oder an geschäftliche Korrespondenz. Durch die Analyse der Art der Kommunikation, insbesondere in Abhängigkeit von bestimmten Faktoren wie z. B. Inhalt, Kommunikationspartner, Wichtigkeit der Kommunikation, persönliche Meinung des Autors zum Inhalt etc., lassen sich nun Aussagen beispielsweise über den Wahrheitsgehalt der entsprechenden Inhalte treffen. Auch daran wird, wie an vielen Big-Data-Anwendungen, zurzeit noch geforscht.[1]

Nach einer repräsentativen Umfrage des Unternehmensverbandes BITKOM aus Mai 2014 verarbeiten die befragten Unternehmen durchschnittlich nur 26 % anonymisierte Daten, wobei sich diese Aussage wohl ausschließlich auf Kundendaten bezieht.[2]

1 Zuständigkeit der Beschäftigtenvertretungen

Je nachdem, ob das Betriebsverfassungsgesetz (BetrVG) oder das Bundespersonalvertretungsgesetz (BPersVG) anwendbar ist, kommen dem Betriebs- bzw. Personalrat umfangreiche Rechte zu. Dabei handelt es sich insbesondere um Informationsrechte (§ 90 BetrVG), Überwachungspflichten (§ 80 Abs. 1 BetrVG, § 68 Abs. 1 BPersVG) und Mitbestimmungsrechte (§ 87 BetrVG, § 75 BPersVG). All diese Vorschriften haben als Anknüpfungspunkt den „Arbeitnehmer“ zum Gegenstand. Eine Zuständigkeit der Belegschaftsvertretungen ergibt sich demnach bei Big-Data-Anwendungen nur, wenn die Daten noch als „Daten der Arbeitnehmer“ in diesem Sinne erkennbar sind. Oder anders ausgedrückt: Handelt es sich nicht um personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG, fehlt es auch regelmäßig an der Zuständigkeit der Belegschaftsvertretungen. Da, wo Big-Data-Anwendungen Daten ohne Personenbezug verarbeiten, ist also für die Mitsprache durch Belegschaftsvertretungen regelmäßig kein Platz, aber auch keine Notwendigkeit. Anonymisierungen von Daten sind allerdings nur ausreichend, wenn eine Deanonymisierung ausgeschlossen ist. Die letzten Jahre haben jedoch gezeigt, dass es immer wieder gelungen ist, anonymisierte Daten zu deanonymisieren und bestimmten Personen zuzuordnen.[3]

1.1 Informationsrechte der Belegschaftsvertretungen

Das in zeitlicher Hinsicht als erstes in Frage kommende Recht bei der Planung von Big-Data-Anwendungen mit personenbezogenen Daten der Beschäftigten ist das Informationsrecht des Betriebsrates. So schreibt beispielsweise § 90 BetrVG vor, dass der Arbeitgeber den Betriebsrat über die Planung von technischen Anlagen „rechtzeitig und unter Vorlage der erforderlichen Unterlagen“ zu unterrichten hat. § 90 BetrVG

ist allerdings nur anwendbar, wenn die geplante technische Anlage, wozu auch DV-Technologien gehören können, dem Arbeitsablauf dient, wobei ausreichend ist, dass dies nur mittelbar geschieht.[4] Ob einzelne Big-Data-Anwendungen mindestens mittelbar einem Arbeitsablauf dienen, kann nicht pauschal beantwortet werden. Dies wird im Einzelfall zu prüfen sein. Wie aber bereits gezeigt, werden einige Big-Data-Anwendungen im betrieblichen Bereich gerade zur Optimierung von Arbeitsabläufen eingesetzt. Zumindest dann haben Big-Data-Anwendungen Einfluss auf Arbeitsabläufe und unterliegen somit der Informationspflicht des § 90 BetrVG. Wichtig bei dieser Vorschrift ist, dass der Arbeitgeber die Belegschaftsvertretung bereits in der Planungsphase „rechtzeitig" zu informieren hat. Die Information muss dabei so frühzeitig wie möglich erfolgen.[5] Der späteste Zeitpunkt ist dabei der, zu dem der Arbeitgeber noch Alternativen überlegt, also noch Einfluss auf die Entscheidung genommen werden kann.[6] Dabei hat die Unterrichtung so zeitig zu erfolgen, dass der Betriebsrat noch in die Lage versetzt wird, eigene Vorschläge und Bedenken zu entwickeln und diese Vorstellungen in den Entscheidungsprozess des Arbeitgebers so einzubringen, dass sie bei der Planung berücksichtigt werden können. Der Betriebsrat ist mithin spätestens dann zu informieren, wenn feststeht, dass Maßnahmen getroffen werden sollen bzw. diese ernsthaft erwogen werden.[7] Dabei ist zu beachten, dass auf den Informations- und Beratungsanspruch des Betriebsrates nicht wirksam verzichtet werden kann. Auch eine Verwirkung dieses Rechtes kommt nicht in Betracht.[8] Die Unterrichtung hat unter Vorlage aller erforderlichen Unterlagen zu erfolgen. Diese hat der Arbeitgeber dem Betriebsrat unaufgefordert vorzulegen.[9] Bei dem Informationsrecht nach § 90 BetrVG handelt es sich mithin nicht um eine Holschuld des Betriebsrates, sondern um eine Bringschuld des Arbeitgebers. Dabei müssen alle wesentlichen Tatsachen, Einschätzungen und Bewertungen grundsätzlich in deutscher Sprache vorgelegt werden.[10]

Wenn im Rahmen der Big-Data-Anwendungen personenbezogene Beschäftigtendaten in der Form verarbeitet werden sollen, dass die Persönlichkeit des Beschäftigten, insbesondere seine Fähigkeiten, seine Leistungen oder sein Verhalten ohne eine gesetzliche Verpflichtung oder ohne dass eine wirksame Einwilligung des Beschäftigten vorliegt, bewertet werden, bedarf die Inbetriebnahme der entsprechenden Anwendung einer Vorabkontrolle im Sinne des § 4d Abs. 5 Nr. 2 BDSG. Gleiches gilt für die Bearbeitung besonders sensibler Daten im Sinne des § 3 Abs. 9 BDSG ohne gesetzliche Notwendigkeit.

Erfüllt der Arbeitgeber seine Informationspflicht überhaupt nicht, unvollständig oder wahrheitswidrig, droht eine Ordnungswidrigkeit nach § 121 BetrVG. Besteht dagegen zwischen dem Arbeitgeber und dem Betriebsrat Streit, ob eine Big-Data-Anwendung überhaupt unter den Anwendungsbereich des § 90 BetrVG zu subsummieren ist, entscheidet das Arbeitsgericht im Beschlussverfahren. Die beharrliche und wiederholte Weigerung des Arbeitgebers, den Betriebsrat trotz einer bestehenden Notwendigkeit rechtzeitig und umfassend zu unterrichten, kann Unterlassungsansprüche gemäß § 23 Abs. 3 BetrVG nach sich ziehen.

1.2 Mitbestimmungsrechte der Belegschaftsvertretungen

Nach § 87 BetrVG und § 75 BPersVG stehen den Belegschaftsvertretungen umfangreiche Mitbestimmungsrechte zu. Das Mitbestimmungsrecht beinhaltet u. a. das Recht, Betriebsvereinbarungen bzw. Personalvereinbarungen mit dem Arbeitgeber bzw. Dienstherrn zu verhandeln und abzuschließen. Gemäß § 87 Abs. 1 Nr. 6 BetrVG und § 75 Abs. 3 Nr. 17 BPersVG besteht ein Mitbestimmungsrecht bei der Einführung und Anwendung technischer Einrichtungen, die „dazu bestimmt" sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen.

DV-Anlagen gehören zu technischen Einrichtungen in diesem Sinne, wobei nach mittlerweile durchgesetzter Meinung auf die Einheit von Rechner und Programm als technische Einrichtung abzustellen ist.[11] Das Vorliegen des Merkmals „technische Einrichtung" wird auch dann zu bejahen sein, wenn bei einem modular aufgebauten EDV-System, welches beim Arbeitgeber bereits vorhanden ist, lediglich ein weiteres Modul, welches nun Big-Data-Anwendungen beinhaltet, hinzugekauft wird.

In der betrieblichen Praxis häufig relevant ist dabei die Frage, inwieweit bloße „Testläufe" oder „Pilotphasen" bereits dem Mitbestimmungstatbestand unterfallen. Häufig wird von Arbeitgeberseite damit argumentiert, dass eine Mitbestimmungspflichtigkeit entfiele, da es sich noch nicht um einen Echtbetrieb, sondern lediglich um einen Testbetrieb handele. Zudem werde das System nur mit einzelnen Daten getestet und noch nicht konzernweit eingesetzt und der Test sei auch nur auf wenige Tage oder Wochen begrenzt.

Zu dieser Argumentation sollte man wissen, dass das Mitbestimmungsrecht unabhängig von einem personellen, räumlichen oder zeitlichen Umfang der jeweiligen Anwendung besteht. Entsprechende Ausschlusstatbestände existieren gerade nicht im Gesetz. Für die Mitbestimmungspflichtigkeit ist es allein erheblich, ob die Softwareanwendung mit echten Daten realer Beschäftigten oder mit Testdaten durchgeführt wird. Wird das System auch nur mit Daten weniger Beschäftigter betrieben, kommt eine Mitbestimmungspflicht in Betracht. Weder der zuständige Betriebsrat noch der Arbeitgeber werden aber zu diesem Zeitpunkt in der Lage sein, eine vollständig ausformulierte Betriebsvereinbarung abzuschließen. Für den Abschluss einer Betriebsvereinbarung relevante Fragen werden sich zu diesem Zeitpunkt des Tests des Systems auch noch gar nicht beantworten lassen. Oftmals dienen Testphasen gerade dazu, die in einer Betriebsvereinbarung zu regelnden Sachverhalte näher zu untersuchen.

Ferner besteht eine Mitbestimmungspflichtigkeit bei diesem Tatbestand nur dann, wenn die DV-Anwendung dazu „bestimmt" ist, das Verhalten oder die Leistung des Arbeitnehmers zu überwachen. Seit langem ist anerkannt, dass eine technische Einrichtung dann zur Überwachung bestimmt ist, wenn sie objektiv dazu geeignet ist.[12] Diese Erkenntnis ist für die Prüfung der Mitbestimmungspflichtigkeit von enormer Wichtigkeit. Häufig vertreten Arbeit-

geber die Ansicht, dass eine Mitbestimmungspflichtigkeit nach diesem Tatbestand nicht vorläge, da sie bestimmte Reporting-Funktionen, die die angeschaffte Software zwar theoretisch bietet, tatsächlich nicht nutzen würden. Dies ist für die Bejahung des Mitbestimmungstatbestandes jedoch unerheblich. Nach der Rechtsprechung des Bundesarbeitsgerichtes (BAG) kommt es lediglich auf die objektive Geeignetheit der technischen Einrichtung an und nicht auf den subjektiven Einsatzwillen oder Einsatzzweck seitens des Arbeitgebers.

Es ist allerdings möglich und empfiehlt sich auch in der entsprechenden Betriebs- bzw. Personalvereinbarung in einer sogenannten Positivliste die Auswertungsmöglichkeiten explizit zu nennen, die tatsächlich auch genutzt werden sollen. So werden die tatsächlich anzuwendenden Überwachungsfunktionen organisatorisch begrenzt.

Fraglich ist demgegenüber auch weiterhin, wann ein Überwachen vorliegt. Nach herrschender Meinung bedeutet „Überwachen“ sowohl das Sammeln von Informationen als auch das Auswerten der Daten.[13] Gegenstand der Überwachung im Sinne dieses Mitbestimmungsrechtes muss dabei das „Verhalten“ oder die „Leistung“ der Beschäftigten sein. Unter „Verhalten“ wird dabei ein individuell steuerbares Tun verstanden. Darüber hinaus wird teilweise verlangt, das Handeln müsse sich auf die Erbringung der Arbeitsleistung beziehen, es müsse im Arbeitsverhältnis und bei der Arbeit erfolgen, außerbetriebliches Tun sei nicht gemeint. Für diese Einschränkung gibt es jedoch keine überzeugende Begründung.[14] Werden durch eine Big-Data-Analyse urlaubsbedingte und krankheitsbedingte Fehlzeiten in Verhältnis zueinander gesetzt, handelt es sich um die Analyse von Verhaltensweisen der Beschäftigten. Wichtig für das Bejahen dieses Mitbestimmungstatbestandes ist, dass die technische Einrichtung, d. h. die DV-Anwendung selbst, die Überwachung bewirkt.[15] Das wird bei Big-Data-Anwendungen immer dann der Fall sein, wenn die der jeweiligen Auswertung zugrunde liegenden personenbezogenen Rohdaten automatisch in eine bestimmte Beziehung zueinander gesetzt werden und diese Beziehung für den Nutzer der DV-Anwendung sichtbar gemacht werden, sei es durch Prozentangaben oder durch die Verwendung grafischer Darstellungen.

1.3 Überwachungspflichten

Gem. § 80 Abs. 1 Nr. 1 BetrVG bzw. § 68 Abs. 1 Nr. 2 BPersVG hat die jeweilige Belegschaftsvertretung darüber zu wachen, dass die zugunsten der Beschäftigten geltenden Rechtsvorschriften, zu denen auch Betriebsvereinbarungen gehören können, eingehalten werden. Aus dem Wortlaut („hat folgende Aufgaben“) wird, deutlich, dass es sich hier nicht um ein Wahlrecht der Belegschaftsvertretung handelt. Ihr steht insofern kein Ermessen zu. Vielmehr handelt es sich um eine gesetzliche Pflicht. Es dürfte sich sogar um eine Garantenpflicht handeln, deren Verletzung strafrechtliche Konsequenzen nach sich ziehen kann. Dies ist bisher für Betriebs- bzw. Personalräte jedoch noch nicht durch die Rechtsprechung geklärt worden.[16] Zu den nach diesen Vorschriften auf ihre Einhaltung zu überwachenden Vorschriften gehören auch die des BDSG.[17]

Die Überwachungspflicht erlischt dabei nicht dadurch, dass im Unternehmen ein betrieblicher Datenschutzbeauftragter bestellt ist, dem ebenfalls durch das BDSG die Überwachung der entsprechenden Vorschriften obliegt.

Im Rahmen der Überwachungspflicht hat die Belegschaftsvertretung umfangreiche Kompetenzen. Insbesondere hat sie Einsichtsrechte, das Recht Auskunftspersonen zu befragen und das Recht, einen Sachverständigen hinzuzuziehen.

Die Überwachungspflicht der Belegschaftsvertretung beginnt mit der Verarbeitung personenbezogener Beschäftigtendaten. Die Pflicht existiert, solange die Verarbeitung erfolgt. Eine abgeschlossene Betriebsvereinbarung lässt die Überwachungspflicht nicht entfallen. Vielmehr hat die Belegschaftsvertretung zudem dann noch die Pflicht, die Einhaltung der Betriebs- bzw. Personalvereinbarung regelmäßig zu überprüfen. Da allerdings der Belegschaftsvertretung nur die Pflicht zukommt, die Vorschriften des BDSG auf ihre Einhaltung hin zu überprüfen, die auch auf die Verarbeitung von personenbezogenen Daten der Belegschaft Anwendung finden, ist auf diese Tatbestände im Folgenden näher einzugehen.

1.3.1. Relevante Vorschriften des BDSG zu Big-Data-Anwendungen

Werden personenbezogene Mitarbeiterdaten für betriebliche Zwecke verarbeitet, besteht regelmäßig kein Zweifel an der Anwendbarkeit des BDSG, § 1 Abs. 2 Nr. 3 BDSG.

1.3.1.1. Die freiwillige Einwilligung als Erlaubnistatbestand für Big-Data-Anwendungen

Fraglich ist, ob ein Beschäftigter in die Verwendung seiner personenbezogenen Daten im Rahmen einer Big-Data-Anwendung „freiwillig“ im Sinne des § 4a BDSG einwilligen kann. In der Regel wird man nicht davon ausgehen können, dass das Bestehen eines sozialen Abhängigkeitsverhältnisses bzw. einer Weisungsgebundenheit, wie sie im Arbeitsverhältnis regelmäßig der Fall ist, generell zu einem Ausschluss der freiwilligen Einwilligung führt. Es bedarf daher besonderer Umstände, um doch noch von einer Freiwilligkeit im Sinne der Vorschrift sprechen zu können. Dies wird in der Literatur etwa dann angenommen, wenn die Eingriffstiefe gering ist oder wenn sich bei objektiver Betrachtung für den Beschäftigten überwiegend Vorteile ergeben.[18] Es hängt daher vom Einzelfall ab, ob Beschäftigte freiwillig in die Verarbeitung ihrer personenbezogenen Daten im Rahmen von Big-Data-Anwendungen einwilligen können. Man wird dies umso eher bejahen können, umso mehr die jeweilige Big-Data-Anwendung als verhältnismäßig angesehen werden kann.

1.3.1.1.1. Direkterhebung der Daten beim Beschäftigten

§ 4 Abs. 3 S. 1 BDSG schreibt vor, dass für den Fall, dass personenbezogene Daten direkt beim Betroffenen erhoben werden, dieser unter bestimmten Voraussetzungen über den Zweck der Verarbeitung seiner Daten zu informieren ist. Dieser Vorschrift kommt im Rahmen von Big-Data-Anwendungen eine besondere Bedeutung zu. Denn

oftmals werden beim Einsatz solcher Anwendungen personenbezogene Daten nicht neu erhoben, sondern es wird mit vorhandenen Datenbeständen, z. B. über Schnittstellen zu anderen Systemen, gearbeitet.

Erfolgte die Information des Beschäftigten über den Verarbeitungszweck der über ihn erhobenen Daten dabei zeitlich vor der Inbetriebnahme der Big-Data-Anwendung, dürfte die alte Zweckdefinition regelmäßig unzureichend sein und muss um die neuen Zwecke ergänzt werden. Die Belegschaft ist insofern unter Umständen nachträglich zu informieren. Dies entspricht auch dem dem BDSG zugrunde liegenden Transparenzgrundsatz, der seinen Ausdruck u.a. in dem Auskunftsrecht gem. § 34 Abs. 1 Nr. 3 BDSG findet.

1.3.1.1.2. Gesetzliche Erlaubnistatbestände für Big-Data-Anwendungen

Als gesetzlich geregelter Erlaubnistatbestand für die Verarbeitung personenbezogener Daten der Belegschaft kommt § 32 Abs. 1 BDSG in Betracht. Danach ist die Verarbeitung zulässig, soweit sie für die verschiedenen Phasen des Beschäftigungsverhältnisses „erforderlich“ ist. In der Literatur wird das Erforderlichkeitskriterium als ein Topos verstanden, welcher einer Abwägung widerstreitender Grundrechtspositionen im Sinne der Herstellung von praktischer Konkordanz den Weg weisen soll.[19] Die Erforderlichkeit wird dabei beispielsweise dann verneint, wenn von mehreren gleich wirksamen Maßnahmen die den Beschäftigten stärker belastende gewählt wurde.[20]

Machen Big-Data-Anwendungen dagegen eine „Übermittlung“ personenbezogener Daten nötig, beispielsweise weil die Anwendung durch einen externen Dienstleister erbracht werden soll, sind dem gegenüber regelmäßig die Erlaubnistatbestände des § 28 Abs. 1 BDSG zu prüfen. Für die Verarbeitung und Übermittlung besonderer Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG gilt der § 28 Abs. 6 BDSG.

Unabhängig davon, welcher Erlaubnistatbestand im Einzelfall tatsächlich greift, kann man von einer Zulässigkeit von Big-Data-Anwendungen aber umso eher sprechen, je mehr diese ausgewogen gestaltet sind und den Rechten der Belegschaft auf Wahrung ihrer Privatsphäre und ihrem Recht auf informationelle Selbstbestimmung Rechnung getragen wird.

1.4. Fazit

Big-Data-Anwendungen mit personenbezogenen Daten unterliegen einer Vielzahl von rechtlichen Rahmenbedingungen. Dies gilt umso mehr für den Fall, dass die entsprechenden Anwendungen in Unternehmen mit Belegschaftsvertretungen eingesetzt werden. Es sollte daher nicht nur aus Gründen der Verhältnismäßigkeit, sondern auch aus Gründen der Praktikabilität zunächst immer versucht werden, Big-Data-Anwendungen mit Daten ohne Personenbezug den Vorrang einzuräumen. Big-Data-Anwendungen mit personenbezogenen Daten sollten die Ausnahme bleiben.

1 http://jetzt.sueddeutsche.de/texte/anzeigen/585271/Ein-Luegendetektor-fuer-Twitter (Zuletzt abgerufen am 11.07.2014.)

2 http://www.bitkom.org/files/documents/Studienbericht_Big_Data_in_deutschen_Unternehmen.pdf (Zuletzt abgerufen am 11.07.2014.)

3 http://www.stanfordlawreview.org/online/privacy-paradox/big-data (Zuletzt abgerufen am 11.07.2014.)

4 Klebe, in: Däubler/Kittner/Klebe/Wedde (Hrsg.), BetrVG, 2012, § 7 Rn. 9.

5 BAG 18.07.72, AP Nr. 10 zu § 72 BetrVG.

6 LAG Hamburg, DB 1985, S. 2308.

7 Klebe, in: Däubler/Kittner/Klebe/Wedde (Hrsg.), BetrVG, 2012, § 7 Rn. 19.

8 Klebe, in: Däubler/Kittner/Klebe/Wedde (Hrsg.), BetrVG, 2012, § 7 Rn. 6.

9 Klebe, in: Däubler/Kittner/Klebe/Wedde (Hrsg.), BetrVG, 2012, § 7 Rn. 22.

10 Klebe, in: Däubler/Kittner/Klebe/Wedde (Hrsg.), BetrVG, 2012, § 7 Rn. 22.

11 Klebe, in: Däubler/Kittner/Klebe/Wedde (Hrsg.), BetrVG, 2012, § 87 Rn. 138.

12 Klebe, in: Däubler/Kittner/Klebe/Wedde (Hrsg.), BetrVG, 2012, § 87 Rn. 154.

13 Klebe, in: Däubler/Kittner/Klebe/Wedde (Hrsg.), BetrVG, 2012, § 87 Rn. 143.

14 Klebe, in: Däubler/Kittner/Klebe/Wedde (Hrsg.), BetrVG, 2012, § 87 Rn. 149.

15 Klebe, in: Däubler/Kittner/Klebe/Wedde (Hrsg.), BetrVG, 2012, § 87 Rn. 153.

16 Zur strafrechtlichen Garantenstellung des Compliance Officers vergl. BGH, BGHSt 54, 44.

17 Buschmann, in: Däubler/Kittner/Klebe/Wedde (Hrsg.), BetrVG, 12. Auflage, § 80 Rn. 10.

18 Däubler, in: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz 2010, § 4a Rn. 23.

19 Seifert, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 2011, § 32 Rn. 11.

20 Gola/Schomerus, BDSG, 2011, § 32 Rn. 12.



Bild: ClipDealer.de

Hans-Hermann Schild

Cloud-Computing aus datenschutzrechtlicher Sicht

1. Was ist Cloud Computing ?

Cloud Computing ist aktuell in aller Munde, doch für die Frage der datenschutzrechtlichen Einordung muss zunächst geklärt werden, was man darunter versteht. Wörtlich übersetzt heißt es nichts anderes als „Datenverarbeitung in der Wolke“. Allgemein ist damit gemeint, dass Hardwarekomponenten und/ oder auch Softwarekomponenten für die gleichzeitige Nutzung mehreren Anwendern zur Verfügung stehen sollen. Im Allgemeinen versteht man darunter ein Konzept, bei dem Speicherplatz und/oder Software nicht mehr auf dem eigenen Rechner, sondern von externen Anbietern bereitgestellt wird.

Dazu zählt auch, dass man sich auf der Geschäftsreise aus der Wolke der dort gelagerten Daten (über das Internet) bedient. Der nachfolgende Beitrag will einen kleinen Überblick zu datenschutzrechtlichen Fragen des Cloud Computings bieten, kann jedoch nicht alle Besonderheiten oder Feinheiten behandeln, die sich allein aus den vielfältigen Angeboten der Cloud ergeben.

Bei der Public Cloud steht das Angebot der Allgemeinheit zur Verfügung (z.B. Google, Amazon, AWS, IBM, …). Bei der Private Cloud stehen die Ressourcen exklusiv für einen Anwender zur Verfügung. Bei der Community Cloud wird diese von Anwendern aus einem Anwendungsbereich genutzt. Demgegenüber besteht die Hybrid Cloud aus mehreren Clouds, bei denen es sich wiederum um Public, Private und Community Clouds handeln kann.

2. Verantwortlichkeit

Wenn Daten an Dritte (Cloud-Betreiber) gehen, ist eins der zentralen Probleme die Datensicherheit, also die Integrität und Vertraulichkeit der Datenverarbeitung für den Cloud-Nutzer. Dabei kann das Argument Sicherheit für einen Cloud-Anbieter sprechen, wenn die IT



Bild: ClipDealer.de

in ein sicheres und geschütztes Rechenzentrum ausgelagert wird. Gleich wie das Vertragsverhältnis für eine Datenverarbeitung in der Cloud im Einzelnen gestaltet ist, ist aber zu beachten, dass sobald personenbezogene Daten verarbeitet werden das Datenschutzrecht anwendbar und für dessen Einhaltung der Datenverarbeiter und damit der Cloud-Nutzer verantwortlich ist. Nach § 3 Abs. 7 BDSG ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. In einem Konzern ist dies das jeweilige Konzernunternehmen (AG, GmbH), d.h. die Mutter und alle Töchter sind zueinander Dritte. Denn ein Konzernprivileg und damit ein Konzerndatenschutzrecht gibt es im europäischen Datenschutzrecht nicht. Die jeweilige verantwortliche Stelle hat die Rechtmäßigkeit der gesamten Datenverarbeitung zu gewährleisten. Dazu zählt auch die Gewährleistung der Rechte des Betroffenen um dessen Daten es sich handelt (Auskunftserteilung – § 34 Abs. 1 BDSG, Löschpflichten – § 35 Abs. 2 BDSG, Sperrung der Daten – § 35 Abs. 3 BDSG, usw.), aber auch jeweils eine Rechtsgrundlage für die Datenerhebung, die Datenverarbeitung (incl. der „Weitergabe“) und die Datennutzung.

Betreibt ein Unternehmen eine eigene Cloud, so ist dies am unproblematischsten, denn das Unternehmen ist als verantwortliche Stelle auch „Herr“ über seine Cloud und kann – ja muss – damit alle notwendigen Schritte und Handlungen. insbesondere auch aus datenschutzrechtlicher Sicht, in eigener Verantwortlichkeit selbst ausüben.

3. Anwendung des Datenschutzrechts

Die datenschutzrechtlichen Regelungen, die es zu beachten gilt, finden immer Anwendung, wenn Daten automatisiert verarbeitet werden, die sich auf eine natürliche Person beziehen oder auf diese beziehbar sind (§ 3 Abs. 1 BDSG). Damit fallen reine Geschäftsdaten einer juristischen Person zwar nicht unter den Anwendungsbereich des Datenschutzrechts. Wenn juristische Personen aber durch natürliche Personen handeln, seien dies Geschäftsführer, Vorstände oder auch nur „Beschäftigte“, so fallen deren Daten als Daten einer natürlichen Person an. Dies mit der Folge, dass Daten der Betroffenen erhoben, verarbeitet und genutzt werden. Dies mit der weiteren Folge, dass – da personenbeziehbare Daten vorliegen – das Bundesdatenschutzgesetz und andere bereichsspezifische datenschutzrechtliche Normen Anwendung finden.

Auch pseudonyme Daten sind personenbezogene Daten. Dabei ist zu beachten, dass auch anonymisierte Daten bei einem entsprechenden großen Aufwand an Zeit, Kosten und Kraft reanonymisiert werden können und damit weiterhin unter den Geltungsbereich des Bundesdatenschutzgesetzes fallen. Auch verschlüsselte personenbezogene Daten bleiben personenbezogene Daten, da sie mit dem entsprechenden Schlüssel wieder entschlüsselt werden können. Damit fallen Lagerverwaltungssysteme,

die sich nur auf Gegenstände beziehen, nicht in den Bereich des Datenschutzrechts. Sowie diese aber auch eine Personenzuordnung (z.B. bei der Auslieferung) enthalten, findet das Datenschutzrecht Anwendung.

Neben dem Bundesdatenschutzgesetz (BDSG) in Deutschland ist auf europäischer Ebene die sog. Datenschutz-Richtlinie 95/46/EG zu berücksichtigen. Sie bildet die Grundlage für das BDSG. Soweit ein öffentlich verfügbarer Telekommunikations-Dienst (z.B. ein E-Mail-Dienst) über eine Cloud-Lösung angeboten wird, ist neben dem BDSG auf europäischer Ebene die Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation, zuletzt geändert durch Richtlinie 2009/136/EG) anwendbar. In Deutschland gilt insoweit dann das Telekommunikationsgesetz (TKG).

4. Auftragsdatenverarbeitung

Während innerhalb der verantwortlichen Stelle die Grundsätze u.a. der Datensparsamkeit (§ 3 a Abs. 1 BDSG), die Verpflichtung zur Meldung der automatisierten Verarbeitung (§ 4d und 4e BDSG), die achte Gebote der Datensicherheit (Anlage zu § 9 BDSG), der Grundsatz der Erforderlichkeit und der Zweckbindung zu beachten sind, wäre bei einer Datenspeicherung außerhalb der verantwortlichen Stelle innerhalb Deutschlands und der EU- bzw. EWR-Staaten darüber hinaus eine Datenverarbeitung im Auftrag gegeben. Dies bedeutet, es gibt einen für die Verarbeitung Verantwortlichen (§ 3 Abs. 7 BDSG), genannt Auftraggeber und einen Auftragnehmer (vgl. § 11 BDSG). Der Auftraggeber ist und bleibt für die Einhaltung der datenschutzrechtlichen Vorschriften und Grundsätze verantwortlich. D.h., der Auftraggeber trägt die Verantwortung für die materielle Zulässigkeit der Datenverarbeitung und haftet gegenüber den Betroffenen (z.B. auf Schadensersatz). Dem Auftraggeber obliegt die Verantwortung für die Einhaltung der Vorschriften über den Datenschutz. Der Auftrag ist schriftlich zu erteilen (siehe auch Art. 17 Abs. 3 RL 95/46/EG). Nach § 11 Abs. 2 BDSG ist im Einzelnen mit dem Auftragnehmer insbesondere schriftlich festzulegen:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Insoweit führt das Institut der Auftragsdatenverarbeitung dazu, dass keine Datenübermittlung an einen Dritten im rechtlichen Sinne erfolgt und bietet damit eine privilegierte Grundlage um sich EDV-mäßig – wenn auch unter Beachtung von Formerfordernissen – innerhalb der EU-Mitgliedsstaaten der Dienste Dritter leichter zu bedienen.

Der Auftraggeber hat sich vor Beginn der Datenverarbeitung von der Einhaltung der getroffenen Maßnahmen nach der Anlage zu § 9 BDSG zu überzeugen, später regelmäßig. Das Ergebnis dieser Überprüfungen ist zu dokumentieren. Ist dies alles erfüllt, so ist die Auftragsdatenverarbeitung auch bei einem Cloud-Anbieter datenschutzrechtlich unbedenklich.

Der Auftragnehmer (Cloud-Betreiber) wäre an die Weisungen des Auftraggebers gebunden. Soweit ein Cloud-Anbieter über ein umfangreicheres Know-How verfügt als der Auftraggeber, müsste er gerade zur Beachtung der Vorgaben des BDSG dem Auftraggeber behilflich sein und die entsprechenden Entwürfe für eine datenschutzgerechte Auftragsdatenverarbeitungsverträge und ggf. auch das Grundgerüst für die Meldung zur Verfügung stellen.

Cloud-Computing-Dienste können jedoch von mehreren Dienstleistern erbracht werden, die als Auftragnehmer bzw. als Unterauftragnehmer tätig werden. Nach Auffassung der sog. Art. 29-Gruppe (ein Gremium, in dem alle Aufsichtsbehörden der Mitgliedstaaten vertreten sind) darf ein Cloud-Anbieter einen Unterauftrag nur mit Einwilligung des Cloud-Anwenders erteilen. Nicht erforderlich ist die Erteilung einer separaten Einwilligung in jedem Einzelfall, eine „generelle Einwilligung" vor Aufnahme der Dienstleistungstätigkeit soll grundsätzlich genügen. Der Cloud-Anbieter ist aber unmissverständlich dazu zu verpflichten, seine Anwender über vorgesehene Änderungen im Hinblick auf den Einsatz neuer oder den Ersatz von Unterauftragnehmern zu informieren. Dabei muss der Cloud-Anwender jederzeit die Möglichkeit haben, den Änderungen zu widersprechen oder den Vertrag zu kündigen. Es sollte eine klare Verpflichtung des Cloud-Anbieters bestehen, alle Unterauftragnehmer zu benennen. Ein von dem Cloud-Anbieter und dem Unterauftraggeber unterzeichneter Vertrag sollte die vertraglichen Regelungen zwischen dem Cloud-Anbieter und der Cloud-Anwender widerspiegeln. Denn was ist, wenn sich der Unterauftragnehmer oder gar die Cloud-Anbieter in einem sogenannten Drittstaat befindet?

5. Drittstaaten

Alle Staaten, die nicht EU-Mitgliedstaaten oder EWR-Staaten (Liechtenstein, Norwegen, Island) sind, sind sogenannte Drittstatten. Eine Datenübermittlung in einen Drittstaat ist nur zulässig, wenn eine Rechtgrundlage zur Datenübermittlung vorliegt (z.B. § 28 Abs. 1 BDSG) und dieser Staat darüber hinaus über ein angemessenes Datenschutzniveau verfügt (§ 4b Abs. 1 Satz 2

und 3 BDSG). Hierunter fallen z.B. die Schweiz, Kanada, Argentinien, Neuseeland, nicht aber die USA. Hier benötigt man für die Datenübermittlung die Genehmigung durch die Aufsichtsbehörde aufgrund ausreichender Garantien oder aber es wurden mit dem Unternehmen im Ausland sogenannte Standardvertragsklauseln (hier gibt es zwei Muster) oder die Standardvertragsklauseln für Auftragsdatenverarbeiter vereinbart (vgl. Art. 26 Abs. 2 EU-DS-RiLi) oder aber das Unternehmen in den USA hat sich den sog. Safe-Harbor-Garantien unterworfen (ein Verfahren, welches mangels Anwendung in den USA in Verruf gekommen ist, siehe aber auch die Vorlage des Irischen High Court vom 18.06.2014 an den EuGH zur Frage der Rechtmäßigkeit des Safe-Harbor-Abkommens) oder es liegen bei einem Konzern verbindliche Unternehmensregelungen (Binding Corporate Rules) vor, die von den Aufsichtsbehörden genehmigt wurden.

Bei einem Drittstaatenbezug zu den USA besteht für die dortigen Behörden immer ein Zugriffsrechts auf die Daten, wie schon die SWIFT-Affäre gezeigt hat. Zwar hat SWIFT, welches den internationalen Zahlungsverkehr abwickelt, seinen Sitz in Belgien, ein Sicherheitsarchiv wird jedoch in den USA betrieben. Dies mit der Folge, dass die Behörden auf diese Daten nach dem Recht der Vereinigten Staaten zugreifen konnten.

Selbst wenn die Daten nicht in den USA, sondern in einem Mitgliedstaat der EU gespeichert sind, ist nicht sicher, dass die US-Regierung nicht ein Zugriffsrecht auf diese Daten geltend macht. Aktuell kämpft Microsoft vor Gericht dagegen, dass in Irland gespeicherte E-Mails an die staatlichen Organe der USA herausgegeben werden sollen (siehe http://www.heise.de/newsticker/meldung/US-Regierung-fordert-Zugriff-auf-Daten-in-EU-Rechenzentren-2260639.html). Denn selbst wenn Daten nur in Europa gespeichert sind, sind sie bei Unternehmen mit Hauptsitz in den USA (wie Microsoft, CSC, IBM, Apple, Cisco usw.) ganz offensichtlich nicht sicher, wenn diese Unternehmen zur Verletzung von Gesetzen eines EU-Landes durch eine amerikanische Gerichtsentscheidung gezwungen würden (Heise Online vom 16.06.2014, http://www.heise.de/newsticker/meldung/Apple-und-Cisco-unterstuetzen-Microsoft-gegen-US-Zugriff-auf-EU-Rechenzentren-2224278.html).

6. Weitere Punkte, die man beachten sollte

Bei dem Einsatz von Cloud Computing sollte sich der Auftraggeber auch die Frage stellen: Wie bleibe ich Herr meiner Daten? Denn nach § 257 HGB ist jeder Kaufmann verpflichtet Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Einzelabschlüsse nach § 325 Abs. 2a HGB, Lageberichte, Konzernabschlüsse, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen, die empfangenen Handelsbriefe, Wiedergaben der abgesandten Handelsbriefe sowie Belege für Buchungen in den von ihm nach § 238 Abs. 1 HGB zu führenden Büchern (Buchungsbelege) geordnet aufzubewahren.

Diese Unterlagen sind zehn bzw. sechs Jahre aufzubewahren. Dabei müssen die Unterlagen während der Dauer der Aufbewahrungsfrist verfügbar sein und jederzeit innerhalb angemessener Frist lesbar gemacht werden können.

Ist dies bei dem Auftragnehmer sichergestellt? Was passiert bei Insolvenz des Auftragsnehmers? Wer ist dann Herr der Daten? Hierzu sollte man bereits vor dem Einsatz von Cloud Computing eine tragfähige Antwort im Sinne des eigenen Unternehmens haben.

Nach § 146 Abs. 2 Satz 1 AO sind Bücher und die sonst erforderlichen Aufzeichnungen im Geltungsbereich der Abgabenordnung (also in Deutschland) zu führen und aufzubewahren. Nur auf schriftlichen Antrag des Steuerpflichtigen kann die Finanzverwaltung bewilligen, dass elektronische Bücher und sonstige erforderliche elektronische Aufzeichnungen oder Teile davon außerhalb des Geltungsbereichs der Abganordnung geführt und aufbewahrt werden können. Diese Bewilligung kann aber jederzeit widerrufen werden. Hat ein Unternehmen seine elektronische Buchführung ohne Bewilligung der zuständigen Finanzbehörde ins Ausland verlagert, kann neben dem sonstigen Werkzeug der Abgabenordnung ein Verzögerungsgeld von 2 500 Euro bis 250 000 Euro festgesetzt werden. Zwar mag eine Bewilligung für das EU-Inland noch zu bekommen sein, es stellt sich jedoch die Frage nach der besonderen Härte, warum die Daten in einem Drittstaat gespeichert werden müssen.

Auch muss für die Datenschutzaufsichtsbehörden die volle Datenschutzkontrolle nach § 38 BDSG möglich sein. Dies wäre bei Auslandsbezug ggf. vertraglich im Benehmen mit der zuständigen Datenschutzaufsichtsbehörde sicherzustellen.

Das Außenwirtschaftsgesetz enthält für Ausfuhren in § 4 AWG Beschränkungen und Handlungspflichten zum Schutz der öffentlichen Sicherheit und der auswärtigen Interessen. Ohne Genehmigung nach § 8 AWG drohen für all die, die einen Verstoß begehen, bußgeldrechtliche und strafrechtliche Sanktionen. Daher ist sicherzustellen, dass durch den Standort des Cloud-Anbieters nicht hiergegen verstoßen wird.

Und ganz zum Schluss: Was passiert, wenn auf den Server des Cloud-Anbieters trotz aller Anstrengungen bei der Datensicherheit unberechtigt zugegriffen wird und Daten des Unternehmens in fremde Hände gelangen? Wie sollen die Kunden, deren Bankdaten entwendet wurden, im Rahmen der Meldepflichten bei Sicherheitsverstößen (siehe § 42a BDSG) informiert werden?

7. Schlussbetrachtung

Auch bei der Cloud gelten neben der Datensicherheit die allgemeinen Regelungen zum Datenschutz. Viele datenschutzrechtliche Forderungen liegen zwar im formalen Bereich, wie die Dokumentation der automatisierten Verarbeitung (Meldung) oder gar die Auftragsdatenverarbeitungsverträge. Diese dienen aber gerade dazu, dass sich die verantwortliche Stelle (das Unternehmen) bereits im Vorfeld ausreichend Gedanken über einen rechtmäßigen Umgang mit personenbezogen Daten macht und nicht erst dann, wenn der Datenschutzskandal passiert ist oder gar gegen Vorgaben der Abgabenordnung verstoßen wurde. Insoweit gehört das Thema Datenschutz auch beim Cloud Computing zu dem Bereich „Governance“, den es zu beachten gilt (in Deutschland spricht man fälschlicher Weise immer von Compliance).

Jonas Plass, Dr. Denis Giffeler

Anti-Doping-Kontrollen mit „eves“

Allein in Deutschland müssen sich etwa 7.000 professionelle Athleten aus unterschiedlichen Sportarten regelmäßigen Dopingkontrollen unterziehen. Zur Anbahnung dieser Kontrollen wird von der Welt-Anti-Doping-Agentur (WADA) ein Programm mit dem Namen Anti-Doping Admission and Administration System (ADAMS) empfohlen. Eingesetzt wird es unter anderem auch in Deutschland.

Die Leistungssportler sind verpflichtet, ihre künftigen regelmäßigen Aufenthaltsorte bis zu drei Monate im Voraus über eine Online-Schnittstelle in ADAMS zu hinterlegen, damit sie bei einer Kontrolle durch den Kontrolleur aufgesucht werden können. Die Pflicht zur Verwendung von ADAMS ergibt sich aus den Regularien der im Internationalen Olympischen Komitee zusammengeschlossenen nationalen Verbände. Zur Bekämpfung des Dopings wurde die WADA 1999 gegründet, deren Vorgaben durch nationale Agenturen umgesetzt werden. In Deutschland ist dies die Nationale-Anti-Doping-Agentur (NADA) mit Sitz in Bonn. Die NADA nutzt das kostenlos bereitgestellte System der WADA, anstatt ein eigenes System zu entwickeln.

Spontane Kontrollen und Doping

Weshalb gibt es überhaupt spontane Wettkampf- und Trainingskontrollen ohne Vorwarnzeit? Dies hängt vor allem damit zusammen, dass Dopingsubstanzen über sehr unterschiedliche Zeiträume im Blut oder in Ausscheidungen nachgewiesen werden können. Außerdem gibt es Möglichkeiten, bestimmte Substanzen durch Einnahme von weiteren Mitteln zu »maskieren«. Oder es wird gleich der ganze Inhalt der Blase gegen Fremd-Urin ausgetauscht. Dem Erfindungsreichtum sind bei der Nachhilfe zur Leistungssteigerung fast keine Grenzen gesetzt. Daher ist es wesentlich, dass Kontrollen möglichst nicht unterlaufen werden können. Und je kürzer die Vorlaufzeit bei Tests ausfällt, desto weniger Zeit bleibt für Gegenmaßnahmen.

Ob die Gestaltung der Kontrollen grundsätzlich den Anspruch an Erforderlichkeit und Angemessenheit im datenschutzrechtlichen Sinne erfüllt, ist nicht Gegenstand der vorliegenden Betrachtung.

ADAMS

Seit seiner Einführung im Jahre 2005 richtet sich die Kritik der Datenschützer in Zusammenhang mit dem System ADAMS insbesondere gegen die folgenden Sachverhalte:

1. Einwilligungsvorbehalt. Die ausschließlich im WADA-Code (und nicht durch nationale Gesetzgebung) festgeschriebene Einwilligung des Athleten in Kontrollen ist Voraussetzung für die Teilnahme an Wettkämpfen. Freiwilligkeit ist demnach nicht gegeben.
2. Datenübermittlung. Persönliche Angaben werden in das zentrale ADAMS nach Kanada übermittelt und können von dort aus weltweit weitergeleitet werden. Es ist offen, ob alle beteiligten Länder über ein Datenschutzniveau verfügen, welches dem der Europäischen Union entspricht. Uns ist nicht bekannt, ob die verantwortlichen Stellen, die ADAMS betreiben oder Sportler zur Nutzung verpflichten, gegenüber den Aufsichtsbehörden Garantien zum Schutz der Persönlichkeitsrechte der Athleten gegeben haben.
3. Dauer der Datenspeicherung. Die Angaben zu Aufenthaltsorten und Erreichbarkeit werden eineinhalb Jahre nach Ablauf der Angaben vorgehalten.
4. Rechte Dritter. Bei der Angabe von Aufenthaltsorten werden – unter Umständen – schutzwürdige Interessen Dritter verletzt, beispielsweise bei Angaben zu Übernachtungsorten.
5. Zweckbindung. Uns ist nicht bekannt, ob von Anti-Doping Organisationen nachgewiesen wurde, dass die erhobenen Daten ausschließlich zum Zwecke von Dopingkontrollen Verwendung finden. Nach EU-Recht ist die Zweckbindung einzuhalten; außerhalb der EU fehlen solche Garantien.

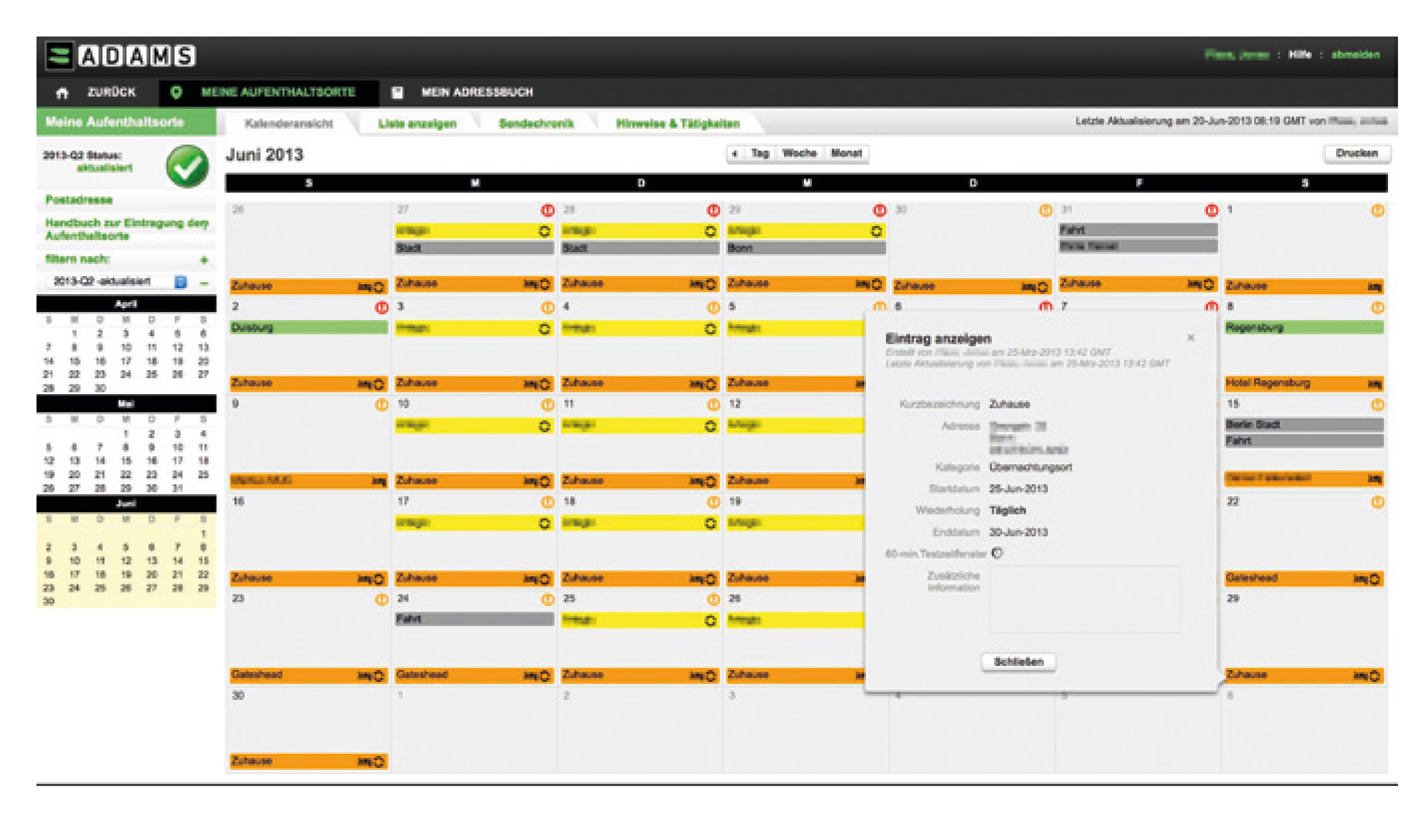
Die Meldepflichten verletzen so möglicherweise auch ganz grundsätzliche Rechte der Sportler wie das Recht auf informationelle Selbstbestimmung, das mit dem angelsächsischen »Right to be left alone« so viel aussagekräftiger bezeichnet ist, sowie Freiheitsrechte wie Versammlungsfreiheit, freie Religionsausübung oder das Demonstrationsrecht.

Diese Unzulänglichkeiten waren Ausgangspunkt für unseren Forschungsansatz zur Schaffung eines – zunächst ergänzenden – Systems für die Ortsbestimmung von Athleten, um die Anbahnung von Dopingkontrollen zu verbessern.

eves

Bei eves handelt es sich um ein aktuelles Forschungsprojekt in der Planungs- und Pilotentwicklungsphase mit dem Ziel, unter Verwendung bewährter und allgemein verfügbarer Ortungstechnologien das Zusammentreffen zwischen Dopingkontrolleur und dem Athleten zu vereinfachen.

Als betroffene Leistungssportler erhoffen wir uns durch den Einsatz von eves einen Zugewinn an persönlicher Freiheit – nicht jede Ortsveränderung muss online angezeigt werden – und durch datensparsamere Meldeerfordernisse einen deutlich verbesserten Schutz unserer Privatsphäre. Für die nationalen und internationalen Anti-Doping-Stellen bedeutet der Einsatz von eves eine Zeitersparnis bei der Anbahnung von



Dopingkontrollen sowie eine erhöhte Akzeptanz bei den Athleten.

eves wird die von dem Athleten in ADAMS hinterlegten Aufenthaltsorte („Whereabouts“) zunächst ergänzen. Wenn Abweichungen zwischen den Ortsangaben und dem tatsächlichen Aufenthaltsort bestehen (z.B. spontane Reiseänderungen bei Streik, Krankheit, familiären Verpflichtungen), soll der Prüfer mit Hilfe von eves den Athleten zukünftig dennoch antreffen können. Für den Athleten bedeutet der Einsatz, dass er sich weniger Sorge um einen fehlgeschlagenen („Missed“) Test machen muss. Denn bei drei „Missed Tests“ droht bislang eine Sperre, auch wenn der Athlet, wie beispielsweise im Fall des Handballers Michael Kraus in diesem Jahr, nicht des Dopings überführt wurde.

Gleichzeitig bedeutet der Einsatz von eves, dass der Athlet nicht von vornherein, aus Angst vor spontanen Aufenthaltsänderungen, potenzielle Aufenthaltsorte in großer Zahl und entgegen der Forderung an Datensparsamkeit in ADAMS hinterlegen muss.

Als wesentliche Komponente von eves wird derzeit ein tragbares Gerät (eves-Client) entwickelt, das speziell an die Bedürfnisse von Athleten angepasst ist. Es ist klein und kann ohne Weiteres jederzeit am Körper getragen werden. Mit seiner Hilfe kann ein autorisierter Doping-Kontrolleur – und nur dieser – bei einer anstehenden Kontrolle den Aufenthaltsort des Athleten ermitteln. Eine Ortung kann nur im Einzelfall durch den berechtigten Kontrolleur vorgenommen werden und sie wird protokolliert. Die Protokolleinträge können durch den Athleten eingesehen werden.

Bei der Entwicklung des eves-Clients stehen folgende Eigenschaften im Vordergrund:

- Lange Batterielaufzeit und -lebensdauer. Das Gerät wird den Träger über eine Statusleuchte informieren, ob ein Fehler vorliegt. Weitere Informationsanzeigen, beispielsweise über den Status einer Abfrage, sind nicht vorgesehen.
- Schutz vor Manipulation. Das Gerät wird über keine externen Schnittstellen verfügen. Das Aufladen erfolgt ohne Steckverbindung durch Induktion. Das Gehäuse ist wasserdicht und vollständig gekapselt.
- Einfache Bedienbarkeit, Selbstbestimmbarkeit und hoher Tragekomfort. Der Athlet kann das Gerät abschalten, beispielsweise wenn er sich in einem Flugzeug oder in einer Klinik befindet.
- Eine Kennzeichnung, um das versehentliche Vertauschen von Geräten zu verhindern.
- Schnelle Ermittlung der Position auch innerhalb von geschlossenen Räumen.
- Sichere und unverfälschbare Übermittlung von Positions- und Statusinformationen ausschließlich zum Zweck der Testanbahnung.

Das tragbare Gerät ermittelt und sendet seinen Standort nur dann, wenn dieser von einem autorisierten Prüfer angefordert wird. Bewegungsprofile können daher nicht erstellt und mithin auch nicht gespeichert werden.

Das eves-System und dessen Kommunikation bauen auf folgenden Komponenten auf:

eves-Client: Das tragbare Endgerät. Nach Empfang einer autorisierten Positionsanfrage über einen dedizierten verschlüsselten Kanal (SMS) prüft es die aktuelle Position mittels Satellitennavigation oder kombinierter Satelliten/Mobilfunk-Ortung (GNSS oder AGPS). Kann keine aktuelle Position bestimmt werden, wird die letzte verfügbare Position oder eine Fehlermeldung auf demselben Weg wie die Anfrage übermittelt. Die letzte verfügbare Position wird in einem internen Speicher für ein Werte-

paar, bestehend aus Längen- und Breitenangabe, vorgehalten.

eves-Server: Ein hochverfügbares System, das in zertifizierten Rechenzentren betrieben wird. Innerhalb des Servers ist den einzelnen Athleten ein eineindeutiges Gerät zugeordnet. Anfragen werden über gesicherte Verbindungen (https) entgegengenommen. Die Weiterleitung der Anfrage erfolgt über SMS an das jeweilige Endgerät. Zurückgeliefert wird die Längen- und Breitenangabe der letzten Position des Athleten oder eine Statusmeldung. Protokolliert werden dabei Zeitpunkt und Autorisierung des anfragenden Prüfers, der Status und die Erreichbarkeit des eves-Clients. Der Athlet hat später die Möglichkeit, auf sämtliche im Zusammenhang mit einer Kontrollanfrage über ihn im System hinterlegten Protokolldaten zuzugreifen. Der Server nimmt auch Meldungen des eves-Clients zum Zustand des Systems, z.B. bei einem kritischen Ladezustand der Batterie, über SMS entgegen.

ADAMS: Enthält unter anderem die Whereabouts der Athleten. Eine technische Anbindung des Systems erfolgt nicht; lediglich der Prüfer kann die Informationen der beiden Systeme abgleichen.

Prüfer: Der Prüfer erhält eine Liste der Athleten, die zu einem bestimmten Zeitpunkt getestet werden sollen. Aus dem ADAMS-System erhält er online Informationen zu den Whereabouts über eine Web-Schnittstelle. Für jeden Athleten dieser Liste kann er eine Anfrage über eine gesicherte Web-Schnittstelle an den eves-Server richten und erhält, sofern verfügbar, die aktuelle Position des Athleten. Diese Positionsangaben kann er über eine Karten-Applikation mit den Whereabouts aus ADAMS vergleichen und so seine Anfahrtswege optimiert planen. Der eves-Server gibt nur in einem begrenzten Zeitraum Angaben zur Position des für einen Test vorgesehenen Athleten. Jede Anfrage wird protokolliert.

Technische und organisatorische Schutzmaßnahmen: Der Betrieb von eves erfordert die Einbettung der technischen Komponenten in einen sicheren Prozess. Auch wenn dieser zum jetzigen Zeitpunkt noch nicht gestaltet werden kann, müssen folgende Rahmenbedingungen für die datenschutzfreundliche Gestaltung auf jeden Fall eingehalten werden:

- Produktion und Ausgabe der Ortungsgeräte müssen manipulationsfrei erfolgen.
- Die Zuweisung eines Prüfauftrags an einen Kontrolleur muss eindeutig und nachvollziehbar erfolgen. Sie darf die einzige Voraussetzung für die Erteilung einer Ortungsbefugnis für den Prüfer bzgl. des zugeteilten Athleten sein. Zuweisung und Ortungsvorgang müssen verfälschungssicher protokolliert werden.
- Die Ortung nicht zu kontrollierender Athleten und die Ortung durch nicht mit der Kontrolle betraute Prüfer muss wirksam unterbunden werden.
- Für abgeschlossene Kontrollvorgänge müssen enge Löschfristen für alle Instanzen von Ortungsergebnissen festgelegt werden.

Zur besseren Übersicht hier nochmals die einzelnen Schritte in der zeitlichen Abfolge:

1. Der Prüfer erhält eine Liste der zu testenden Athleten.
2. Er ermittelt die Whereabouts der Athleten mit Hilfe von ADAMS.
3. Vor der Anfahrt stellt er, via Web-Zugriff, eine Positionsanfrage an den eves-Server.
4. Der eves-Server leitet die Anfrage, sofern zulässig, als SMS an den eves-Client weiter.
5. Der eves-Client ermittelt, sofern zulässig, die letzte Position und leitet diese per SMS an den eves-Server.
6. Der eves-Server liefert die Ergebnisse der Rückmeldung des eves-Clients an den Prüfer und protokolliert den Abschluss der Anfrage ohne Positionsangabe.

Aktueller Status: Testphase

Derzeit laufen die Vorbereitungen für einen Feldtest, bei dem die folgenden Fragestellungen in Hinblick auf Sicherheit, Nachhaltigkeit, initiale und laufende Kosten sowie technische Machbarkeit untersucht werden.

1. Welche Methoden der Positionsbestimmung erlauben eine ausreichend genaue Lokalisierung in unterschiedlichen Alltagssituationen (u.a. GPS / GNSS, GSM-Triangulation, WLAN, RF);
2. Welche Kommunikationswege genügen den hohen Anforderungen an Vertraulichkeit und Integrität der Daten (z.B. GSM, GPRS, WLAN);
3. Weitere Randbedingungen wie Gebrauchstauglichkeit und Tragekomfort im Alltag, Batterielaufzeit, Material- und Umweltverträglichkeit, Transport und Logistik etc.

Die wesentlichen Rahmenanforderungen in Bezug auf Datenschutz wurden bereits formuliert. Sie weiter zu detaillieren und in die Prozesse zu implementieren ist der nächsten Projektphase vorbehalten, wenn der Test eine grundsätzliche Machbarkeit ergeben hat.

Der Test ist ergebnisoffen angelegt mit dem Ziel einer Gesamtlösung, die in Bezug auf Sicherheit, Nachhaltigkeit und Kosten optimiert ist. Sollte keine signifikante Verbesserung der Testanbahnung zwischen Athleten und Prüfer zu beobachten sein, bleibt zu prüfen, ob der Zugewinn an persönlicher Freiheit und verbessertem Schutz der Persönlichkeitsrechte der Athleten den Einsatz dennoch rechtfertigen.

Sicherheit

- In Anlehnung an den IT-Grundschutz und unter Beachtung weiterer Prüfkataloge wie z.B. OWASP werden, gemeinsam mit dem Fraunhofer Institut AISEC, die Komponenten des Gesamtsystems auf mögliche Gefährdungen untersucht und Risiken bewertet. Dabei geht die Betrachtung über die rein technischen Aspekte hinaus, indem auch elementare Gefährdungen, höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen und vorsätzliche Handlungen als Risiken betrachtet werden.

Neben der rein technisch/fachlichen Ausrichtung ist eines der Hauptziele des Forschungsprojektes die Verbesserung der datenschutzrechtlichen Belange der Athleten. Die fachliche Begleitung und Dokumentation des Projekts durch die jeweiligen Experten soll die notwendige Transparenz von eves sicherstellen. Wir hoffen zudem, dass die Ergebnisse aus dem Projekt letztlich für mehr Rechtssicherheit sorgen, wenn die Politik die zu erwartenden Ergeb-

nisse aus dem Projekt in die aktuelle Gesetzgebung einfließen lässt.

Die Athleten

Seit wir uns intensiv mit der Problematik auseinandersetzen, ist uns eines bewusst geworden: Fast jeder hat eine Meinung, wenn es um Doping geht. Bei den Athleten als den in besonderer Weise Betroffenen ist diese verständlicherweise durch den Wunsch geprägt, möglichst wenig „Ärger" mit den Doping-Kontrollen zu haben. Würden die Athleten eves als Erleichterung empfinden, so wie wir dies beabsichtigen?

Um dies herauszufinden, wurde im Oktober 2014 gemeinsam mit der NADA und dem Deutschen Olympischen Sportbund eine anonyme Befragung unter 800 Leistungssportlern und 90 Prüfern durchgeführt. Unter anderem waren sämtliche Olympiateilnehmer des Deutschen Teams aus Sotchi und London beteiligt. Die Auswertung hat ergeben, dass der überwiegende Teil beider Gruppen die Einführung eines Systems wie eves begrüßen würde.

Im Rahmen dieser Untersuchung wurden wir allerdings auch mit einigen typischen Fragen konfrontiert, die von den Athleten aufgeworfen wurden. Sie zeigen, dass Athleten neben dem Wunsch, „Ärger" mit den Doping-Kontrolleuren zu vermeiden, einerseits sehr wohl zu Kompromissen bereit sind, andererseits aber keine unbeschränkte Überwachung akzeptieren und ihr informationelles Selbstbestimmungsrecht erfreulich hoch bewerten. Wir dokumentieren einige der aufschlussreichen Fragen und unsere Antworten an dieser Stelle.

A: Wo ist der Unterschied zu einer elektronischen Fußfessel?

S: Die Teilnahme an eves ist freiwillig. Das System ergänzt die Ortsangaben, die in ADAMS vom Athleten hinterlegt werden. Im Gegensatz zur Fußfessel sendet und speichert eves grundsätzlich keine Daten. Es wird nur ausnahmsweise aktiv und ermittelt und sendet die Position, wenn es über eine sichere Verbindung zur Anbahnung einer Prüfung von autorisierten Personen dazu aufgefordert wird.

A: Ich besitze doch schon ein Smartphone – weshalb also keine App?

S: Das hat mehrere Gründe. Selbst wenn die App vorbildlich programmiert wäre, könnte nicht sichergestellt werden, dass andere Anwendungen nicht auch auf die App zugreifen. Nur der Prüfer darf jedoch die Ortsangabe erhalten, ohne dass weitere Personen dies mitbekommen – auch nicht der Athlet selbst.

A: Ich kenne meine Rechte. Wie erfahre ich, was eves über mich speichert?

S: Auf einem Server in Deutschland ist jedem Athleten eine Nummer zugeordnet. Über diese Nummer kann der Server mit dem Gerät Kontakt aufnehmen. Er erhält dann den Ort, den das Gerät im Augenblick der Abfrage ermittelt und leitet diesen an den Prüfer weiter. Der Athlet kann nach einer durchgeführten Kontrolle selbst prüfen, wann eine Ortsabfrage erfolgte, indem er die Protokolldatei einsieht. Die Orte selbst werden nicht gespeichert.

A: Was hat Priorität: Die Ortsangabe in ADAMS oder die von eves ermittelte Position?

S: Wenn der Athlet nicht angetroffen wird, erhält er, wie bisher auch, Gelegenheit zu einer Stellungnahme. Im Zweifelsfall wird zu Gunsten des Athleten entschieden.

Was kommt als Nächstes?

Aktuell ist das eves Team bestehend aus Athleten, der Nationalen Anti-Doping Agentur NADA, dem Fraunhofer Institut AISEC, Datenschützern, Systemanalytikern und Hardware-Spezialisten in der Vorbereitung auf einen Feldtest mit Freiwilligen aus unterschiedlichen Sportarten. Dort soll die Gebrauchstauglichkeit des Systems im Alltag getestet und Rückschlüsse für den sicheren Dauerbetrieb gezogen werden. Die Forderung nach Verfügbarkeit, Integrität, Vertraulichkeit und Verbindlichkeit einerseits und Transparenz, Intervenierbarkeit und Nichtverkettbarkeit andererseits der personenbezogenen Daten ist dabei für alle Projektbeteiligten oberstes Ziel.

In Politik und Öffentlichkeit scheint immer noch die Meinung vorzuherrschen, dass jeder Profi-Sportler nur durch die Anti-Doping-Kontrollen abgehalten wird, seine Leistungen mit unerlaubten Mitteln zu steigern. Das ist falsch. Die Athleten unterziehen sich dem harten Anti-Doping-Regime, um gleiche und faire Bedingungen für alle zu erhalten.

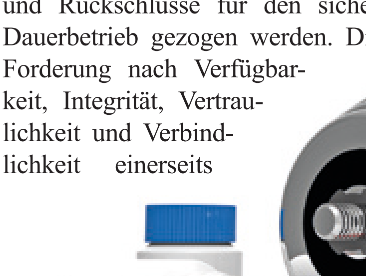
Es gilt, die Athleten in Fragen der Verwendung und Schutz ihrer Daten zu sensibilisieren. Und es gilt den immer subtileren Methoden der Betrüger etwas entgegenzusetzen.

Es hat hier überrascht, dass es das ADAMS System bislang noch nicht auf die Negativ-Liste des Big Brother Awards (https://www.bigbrotherawards.de/archive) geschafft hat.

Wir sind uns darüber im Klaren, dass, durch eine Ergänzung von ADAMS durch eves, die bestehenden datenschutzrechtlichen Mängel nicht behoben sind. Jedoch möchten wir in einem ersten Schritt aufzeigen, dass sich das Ziel der unangekündigten Trainingskontrollen mit entsprechenden datenschutzkonformen Mitteln sogar effektiver und effizienter erreichen lässt. Sobald hierfür ein Bewusstsein bei den verantwortlichen Institutionen geschaffen ist, muss die Sinnhaftigkeit einer weiteren Pflege der Whereabouts hinterfragt werden.

Wer weiß – vielleicht löst Eva ja eines Tages Adam ab?

Bild: ClipDealer.de





Arnold von Bosse

Verfassungsbeschwerde gegen das Bestandsdaten-Auskunftsgesetz Mecklenburg-Vorpommern

Das heimliche Abrufen von elektronisch generierten Telekommunikations-Daten durch Verfassungsschutz und Polizei ist im Telekommunikationsgesetz des Bundes (TKG) und in den entsprechenden Landesvorschriften normiert. Wie wird hier die Balance zwischen Sicherheitsinteressen auf der einen Seite und Schutz der Intimsphäre auf der anderen Seite austariert?

Immerhin geht es einerseits z.B. um das Verhindern eines im Internet angekündigten Selbstmordes oder Amoklaufes, andererseits um die Missbrauchsgefahr, die im staatlich erfolgten Abruf tausendfacher Zugangssicherungscodes (PIN, PUK, Passwörter, Zugang zu E-Mail-Konten oder Cloud-Speichern) liegen kann.

Um das zu überprüfen, ist im Juni 2014 eine durch die Partei Bündnis 90/Die Grünen initiierte Verfassungsbeschwerde beim Landesverfassungsgericht Mecklenburg-Vorpommern in Greifswald eingelegt worden. Der sperrige Name des angegriffenen Gesetzes: „Gesetz zur Änderung des Landesverfassungsschutzgesetzes und des Sicherheits- und Ordnungsgesetzes zur Regelung der Bestandsdatenauskunft v. 2.7.2013“ (Lt-Drucksache 6/1630) – kurz: Bestandsdaten-Auskunftsgesetz M-V (siehe Auszug im grauen Kasten).

Dabei ist schon der Name irreführend und verharmlosend: „Bestandsdaten“ sind z.B. die Adress- und Vertragsdaten (Kundendaten im Sinne der §§ 95, 111 TKG der Telekommunikations-Dienste-Anbieter (Provider)). Diese Daten sind am wenigsten schützenswert und nicht Gegenstand der verfassungsrechtlichen Kritik: Eigentlich hätte das Gesetz „Inhalts- und Verkehrsdaten-Auskunftsgesetz“ heißen müssen. Denn diese Daten sind es, die die geschützte Intimsphäre offen zu legen in der Lage sind: Weil nämlich indirekt durch das im angegriffenen Gesetz erlaubte Abrufen von Zugangssicherungscodes von Handys und Computern auch Inhaltsdaten, z.B. durch Bewegungsprofile, sichtbar werden. Die zweite Daten-Kategorie im angegriffenen Gesetz sind die Verkehrsdaten, zu denen die „dynamischen Internet-Protokoll-Adressen (IP-Adressen)“ gehören. Diese werden dem Internet-Nutzer immer wieder neu beim Aufschlagen einer Homepage zugeordnet: Auch hier sind Rückschlüsse auf Inhalte möglich.

Im Folgenden sollen die wesentlichen Angriffspunkte der Beschwerde aufgezeigt werden. Motivation der Beschwerde war, dass das o.g. Landesgesetz bzgl. des Schutzes der persönlichen Verbindungsdaten hinter ähnlichen Gesetzen aller anderen Bundesländer und des Bundes zurück bleibt.

Die Verfassungsbeschwerde macht geltend, dass die neuen, zum 1.7.2013 in Kraft getretenen Vorschriften des Bestandsdaten-Auskunftsgesetz M-V mit Verweis auf das Landesverfassungsschutz-Gesetz M-V (LVerfSchG) und das Sicherheits- und Ordnungs-Gesetz M-V (SOG) gegen das Datenschutzgrundrecht aus Art. 6 (1) Landesverfassung M-V (LV) und die Rechtsschutzgarantie (Art. 19 (4) Grundgesetz) verstoßen und daher nichtig sind.

Art. 6 (1) LV lautet:
„Jeder hat das Recht auf Schutz seiner personenbezogenen Daten. Dieses Recht findet seine Grenzen in den Rechten Dritter und in den überwiegenden Interessen der Allgemeinheit.“

Art. 6 (1) LV als Datenschutzgrundrecht findet seine Inhaltsbestimmung auch in Art. 10 GG (Fernmeldegeheimnis) und im informationellen Selbstbestimmungsrecht (Art. 2 (1) i. V. m. Art. 1 (1) GG sowie in der speziellen Ausprägung als „Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“.

Die verfassungsrechtlichen Prüfgrundsätze ergeben sich dabei vor allem
- aus dem sog. Vorratsdatenurteil des Bundesverfassungsgerichts (BVerfG) v. 2.3.2010 (1 BVR 256/08)
- und aus dem Beschluss des BVerfG v. 24.1.2012 (1 BVR 1299/05) zur Verfassungswidrigkeit des Abrufes von Daten zu Zugangssicherungs-Codes von Mobiltelefonen und Computern und der Daten zu dynamischen IP-Adressen. Die untenstehend geprüften Landesgesetzes-Änderungen sind in Folge dieser Entscheidung ergangen, um den strengen Vorgaben des BVerfG Genüge zu tun. Diese Vorgaben sind aber im Bestandsdaten-Auskunftsgesetz M-V aus Sicht der Beschwerdeführer (und des Autors, der der Verfasser der Beschwerdeschrift ist) nicht erfüllt.

I. Zum neuen § 24b LVerfSchG

Das Landesverfassungsschutz-Gesetz erlaubt u. a. die vorbeugende Sichtung von Gefahren für den Staat und die Benachrichtigung der Regierung über verfassungsrechtlich relevante Einschätzungen durch den Landesverfassungsschutz.

1. Zur Berechtigung bzgl. des Abrufes von Zugangssicherungs-Codes

a. Die sog. Bestimmtheit der gesetzlichen Regelung, die für den Datenabruf gemäß der Schwellen-Vorgaben des Grundrechts auf Datenschutz in Art. 6 LV-MV gefordert wird, ist unzulänglich: Denn die Zwecke des Abrufes der Daten sind nicht normiert. Die vom BVerfG geforderte Normenklarheit fehlt: Der bloße Verweis auf die „gesetzlichen Voraussetzungen“ reicht nicht. Weder der Bürger, der Anspruch auf Rechtsschutz hat (Art. 19 (4) GG) noch der einfache Poli-

zeibeamte haben im Alltag Kenntnis, welche Vorschriften sich dahinter verbergen.

b. Die Normierung der nachträglichen Mitteilungspflichten, nachdem die Daten zu den Codes abgerufen wurden, fehlt. Sucht man danach, findet man zwar § 2 im Gesetz zur Ausführung des Art. 10-Gesetzes, GVBl.M-V 1992, 486 (Gesetz zur Kontrolle des Verfassungsschutzes, wenn in das Telekommunikations-Geheimnis aus Art. 10 GG eingegriffen wird).

Hier wird aber nur die Pflicht zu Mitteilungen für den Abruf von Daten bei laufender Telekommunikation geregelt. Bzgl. der bereits abgelegten Daten (z.B. auf Mobiltelefonen, wenn das „surfen" beendet ist) gibt es keine nachträglichen Mitteilungspflichten.

Der Eingriff in die Privatsphäre hat aber bzgl. des Abrufes von Daten aus laufender und abgeschlossener Kommunikation eine ähnliche Intensität. Das Fehlen dieser Mitteilungspflichten führt zur Verfassungswidrigkeit von § 24b LVerfSchG bzgl. dieses Aspektes, da der Betroffene nach dem heimlichen Abruf der Daten aufgrund Nichtwissens sich nicht wehren kann (Verstoß gegen Art. 6 LV und Art. 19 (4) GG gem. dem vom BVerfG entwickelten Gebot des „effektiven Rechtsschutzes").

c. Es stellt einen verfassungsrechtlichen Mangel dar, dass ein sog. Richtervorbehalt (also die Vorab-Genehmigung vor dem Eingriff in die Privatsphäre) weder für den Abruf von Daten zur laufender Kommunikation noch beim Abruf von abgelegten Daten geregelt ist.

Im Polizeirecht (beim Drohen von Gefahren, siehe unten) gibt es jedoch den Richtervorbehalt zumindest beim Abruf der Daten zu laufender Kommunikation. Es wäre daher auch im Rahmen der bisherigen landesgesetzlichen Systematik konsequent, dies auch im Verfassungsschutzrecht vorzusehen.

Der Richtervorbehalt ist bei erheblichen Eingriffen verfassungsrechtlich geboten. Gewichtige Stimmen von Verfassungsrechtlern (siehe unten zur Literatur/Stellungnahmen) sind der Auffassung, dass der Richtervorbehalt geboten ist, da es sich beim Abruf von Daten zu Codes und IP-Adressen um intensive Eingriffe in die Privatsphäre handelt. Denn aus den sog. Verkehrsdaten kann oft auch – wie oben dargelegt – auf die Inhalte und schützenswerte persönliche Vorlieben geschlossen werden. Der Richtervorbehalt wird weiter unten nochmals thematisiert.

2. Zur Berechtigung bzgl. des Abrufes von Daten zu dynamischen IP-Adressen

a. Die Bestimmtheit fehlt auch hier, die bloße Bezugnahme auf das Bundesgesetz (§ 113 TKG) reicht nicht. Bei Eingriffen in Grundrechte, z.B. Art. 6 LV, müssen die Voraussetzungen des Eingriffes möglichst genau geregelt sein, damit dem Willkür-Verbot aus Art. 20 (3) GG Genüge getan wird. Auch der Europäische Gerichtshof hat am 8.4.2014 (C-293/12 und C-594/12) den Datenschutz gestärkt, indem er forderte, dass klare Schranken bzgl. des Abrufes von privaten Daten normiert werden (Verhältnismäßigkeits-Grundsatz).

b. Mitteilungspflichten sind (im Gegensatz zu den abgelegten Daten zu Codes) beim Abruf der Daten zu dynamischen IP-Adressen im neuen § 24b des LVerfSchG erfreulicherweise geregelt. Allerdings fehlt auch hier der Richtervorbehalt.

II. Zu § 28a SOG M-V

Das Sicherheits- und Ordnungs-Gesetz betrifft das Handeln der Landespolizei beim Drohen von Gefahren für die öffentliche Sicherheit und Ordnung (z.B. Ankündigung von Stalking oder einem Amoklauf im Internet).

1. Abruf von Zugangssicherungscodes

a. Die Bestimmtheit der Regelung des Abrufes der Codes ist auch hier nicht ausreichend. Der Begriff „konkrete" Gefahr fehlt (Vorgabe des BVerfG). Es wird keine Eingrenzung auf nur „gewichtige Ordnungswidrigkeiten" vorgenommen (Vorgabe des BVerfG). Der bloße Verweis auf die „gesetzlichen Voraussetzungen" reicht nicht.

b. Nachträgliche Mitteilungspflichten sind zwar in § 34a (7) SOG geregelt; dies gilt aber nur für den Abruf von Daten zu laufender Kommunikation. § 28a SOG ist also insofern verfassungswidrig, als die Normierung von Benachrichtigungs-Pflichten nach dem heimlichen Abruf von abgelegten Daten fehlt.

c. Sucht man den Richtervorbehalt, so findet man ihn in § 34a (4) SOG. Aber dieser gilt nicht für den Abruf von schon abgelegten Daten. Die Eingriffsintensität in die Privatsphäre ist aber die gleiche wie bei laufender Kommunikation. § 28a SOG ist also bzgl. dieses Aspektes verfassungswidrig, da die aufgrund des Datenschutzgrundrechts in Art. 6 LV notwendige Schwelle des Richtervorbehaltes als einzelfallbezogene Grundrechtssicherung bei abgelegten Daten fehlt.

2.Abruf von Daten zu dynamischen IP-Adressen

a. Die Bestimmtheit reicht nicht; der genaue Zweck ist nicht benannt, siehe oben.

b. Auch hier fehlt nach Auffassung der Beschwerdeführer der Richtervorbehalt. Allerdings widerspricht sich das BVerfG in seiner o.g. Vorratsdaten-Entscheidung selber (mal wird ein intensiver Eingriff in die Intimsphäre angenommen (Rz. 211), mal wird der Richtervorbehalt mit der Begründung abgelehnt, es handele sich nicht um eine große Eingriffsintensität (Rz. 261)). Zudem formulierte das BVerfG, IP-Adressen seien zwar Verkehrsdaten, aber sie seien nicht so eingriffsintensiv wie bei anderen Verkehrsdaten, da die Verwendung nur „mittelbar" erfolge (Vorratsdaten-Urteil, Rz. 254).

Bzgl. dieses Widerspruchs im Vorratsdaten-Urteil des BVerfG befragte der Verfasser der Beschwerdeschrift den Datenschutzbeauftragten von Berlin, Dix. Dieser antwortete am 15.4.2014 wie folgt:

„Das Gericht hatte in der Vorratsdaten-Entscheidung die Tragweite der IP-Adresse als „Generalschlüssel" zum Kommunikationsverhalten der Internet-Nutzer verkannt (trotz entsprechender Hinweise der Sachverständigen in der

mündlichen Verhandlung). Praktisch läuft die Personalisierung der IP-Adressen so, dass eine Strafverfolgungsbehörde, die IP-Adressen hat, zunächst bei der Bundesnetzagentur nachfragen muss, welcher Provider den entsprechenden Block an IP-Adressen vergeben hat. Der jeweilige Provider teilt der Strafverfolgungsbehörde (oder Gefahrenabwehr-Behörde – Einschub durch Verfasser) dann mit, welchem Nutzer eine bestimmte (meist dynamische, selten statische) IP-Adresse zugewiesen war, wenn der Provider die Daten noch hat (noch nicht gelöscht hat). Dieser Prozess hat offenbar das BVerfG zur Wahl des Attributs „mittelbar“ veranlasst.“

Es spricht also vieles dafür, die Eingriffsintensität bzgl. des Abrufes von dynamischen IP-Adressen als intensiv einzuordnen – mit der Folge der Notwendigkeit eines Richtervorbehaltes.

Abschließend sei angemerkt, dass die Relevanz der „Bestandsdatenauskunft“ nicht zu unterschätzen ist: Immerhin erfolgten 2013 bundesweit durch die Behörden z.B. allein von Google 6000 und von Facebook 4000 Datenabrufe (Transparenz-Berichte 5.5.2014). Im Übrigen muss die Entwicklung der sog. statischen IP-Adressen (Version 6) beobachtet werden, da die technische Entwicklung diesbezüglich zu einem noch tieferen Eingriff in die Privatsphäre führen kann, als bisher vorstellbar. Auch daher bietet es sich an, die Eingriffs-Schwellen-Voraussetzungen als Verfahrenssicherung vorsorglich nicht zu niedrig anzusetzen, um nicht alle 2 Jahre die Gesetze an die rasanten technischen Entwicklungen anpassen zu müssen.

Literatur, Stellungnahmen und ein weiteres Urteil zu der obigen Problematik:

Roggenkamp, Neuregelung zur Bestandsdatenauskunft verfassungswidrig!, NJW-aktuell 21/2013, S. 12

Kugelmann, Dalby, Die Neuregelung der Bestandsdatenauskunft gem. § 113 TKG und die Notwendigkeit des Grundrechtschutzes durch Verfahren, Festschrift für Kutscha, Das Recht in guter Verfassung?, 2013, 114 (Kugelmann gab auch eine ähnlich lautende Stellungnahme im Gesetzgebungsverfahren in M-V ab).

Gusy, Stellungnahme v. 2.5.13 zur Anhörung bzgl. der Änderung des Polizeigesetzes NRW – LT-Drs. 16/2256

Neue Richtervereinigung Schleswig-Holstein, Stellungnahme v. 3.6.2013 zur Anpassung des manuellen Abrufs der Bestandsdaten nach dem TKG, LT-Dr. 18/1713

Albrecht, Stellungnahme v. 8.5.2013 zur Anhörung zum Gesetz zur Änderung des Polizeigesetzes NRW, LT-Drs. 16/2256

BVerfGE 120, 274 (Online-Durchsuchung)

Verfassungsgerichtshof Thüringen, Urteil v. 21.11.2012 (VerfGH 19/09)

Die Verfassungsbeschwerde ist unter www.bestandsdatenauskunft-mv.de abrufbar.

Auszug

§ 24b LVerfSchG M-V
Gesetz über den Verfassungsschutz im Lande Mecklenburg-Vorpommern (Landesverfassungsschutzgesetz – LVerfSchG M-V)
Quelle: http://www.lexsoft.de/cgi-bin/lexsoft/justizportal_nrw.cgi?t=141145570986982651&sessionID=2093881221810774250&source=link&highlighting=off&templateID=document&chosenIndex=Dummy_nv_68&xid=188081,35

Abschnitt: Abschnitt 3 – Informationsübermittlung und Auskunftserteilung
§ 24b LVerfSchG M-V – Weitere Auskunftsverlangen

(1) Soweit dies zur Erfüllung der Aufgaben der Verfassungsschutzbehörde erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, im Einzelfall Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 1 des Gesetzes vom 20. Juni 2013 (BGBl. I S. 1602) geändert worden ist, erhobenen Daten verlangt werden (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes). Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes).

(3) Von einer Beauskunftung nach Absatz 2 ist die betroffene Person zu benachrichtigen. …

Auszug

§ 28a SOG M-V
Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern (Sicherheits- und Ordnungsgesetz – SOG M-V) – Landesrecht Mecklenburg-Vorpommern
Quelle: http://www.lexsoft.de/cgi-bin/lexsoft/justizportal_nrw.cgi?t=141145552983903551&sessionID=2093881221810774250&chosenIndex=Dummy_nv_68&templateID=document&source=context&source=context&highlighting=off&xid=188215,129

Abschnitt: → Unterabschnitt 1 – Datenerhebung
§ 28a SOG M-V – Erhebung von Telekommunikationsdaten im manuellen Auskunftsverfahren

(1) Die Polizei kann zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 1 des Gesetzes vom 20. Juni 2013 (BGBl. I S. 1602) geändert worden ist, erhobenen personenbezogenen Daten verlangen (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes). Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes). In diesem Fall ist die betroffene Person über die Beauskunftung zu unterrichten. …

Moritz Eggert

„Ich akzeptiere die Nutzungsbedingungen“

Bericht von der Uraufführung einer Vertonung der Nutzungsbedingungen von Google

Es geschieht immer wieder, dass man als Komponist gebeten wird, ein Stück für eine Feierlichkeit zu komponieren. So bat mich die Goethe-Universität Frankfurt am Main, zu ihrer 100-Jahr Feier eine Komposition beizutragen.

Ein Stück zum Jubiläum der Goethe-Universität Frankfurt zu komponieren beinhaltet die Verantwortung, dem Namen und der Bedeutung dieser Universität gerecht zu werden. Doch wie erreicht man dies? Naheliegend erschien mir zuerst, einen Text von Goethe zu vertonen: etwas Schönes, Festliches, zum Anlass Passendes. Man hätte danach gerührt und ergriffen einander die Hände schütteln und wieder zur Tagesordnung übergehen können.

Doch dann dachte ich mir, dies wäre es sich zu leicht gemacht, angesichts der politischen und oft progressiven Rolle, die diese Universität in der Vergangenheit gespielt hat; vor allem, da man bei einem Jubiläum doch eher in die Zukunft blicken sollte, anstatt sich auf den Lorbeeren der Vergangenheit auszuruhen.

Deswegen fand ich es schließlich passend, eines der großen Themen unser aller Zukunft (und natürlich Gegenwart) in den Mittelpunkt meiner Komposition zu stellen, nämlich den zunehmenden und größtenteils von uns freiwillig in Kauf genommenen Verlust von Freiheit in der digitalen Welt.

Stellen Sie sich vor, Sie gehen in eine Bäckerei und kaufen ein Stück Brot. Doch bevor Ihnen der Bäcker das Brot verkauft, will er alles Mögliche von Ihnen wissen: Wie Sie heißen, wo Sie wohnen, wie alt Sie sind. Ihr Beruf, Ihre Hobbies, alle Ihre Interessen. Welche Freunde Sie haben, wo Sie gerade herkommen, wohin Sie gereist sind, wohin Sie reisen werden. Welcher Schicht Sie angehören, wieviel Sie monatlich verdienen, für was Sie in der letzten Zeit Geld ausgegeben haben, und für was Sie Geld auszugeben gedenken. Was Sie sich gerne anschauen, welche Filme Sie mögen, welche Bücher Sie lesen, was Ihre politische Gesinnung ist, welche sexuellen Vorlieben Sie haben, ob Sie heterosexuell, homosexuell oder bisexuell sind, ob Sie verheiratet sind oder ledig, wie viele Kinder Sie haben, was diese Kinder machen, wo sie zur Schule gehen, wo sie studieren. Und das ist nur der Anfang einer langen Liste von Fragen, die Ihnen der Bäcker stellt.

Nachdem Sie all diese Fragen beantwortet haben (und der Bäcker erkennt, wenn Sie lügen, weil er bereits Informationen über Sie von anderen Bäckern, Metzgern und Obsthändlern erhalten hat – also müssen Sie die Wahrheit sagen), hält Ihnen der Bäcker ein Dokument hin, das Sie unterschreiben müssen. In diesem Dokument steht, dass der Bäcker all die Informationen, die Sie ihm gerade gegeben haben, beliebig weiterverwenden, speichern und vor allem an Dritte weitergeben kann, wie es ihm beliebt. Er kann Ihnen von nun an alles vorschlagen, was Sie in Zukunft kaufen sollen, er kontrolliert, welche Waren Ihnen beim nächsten Einkaufsbummel präsentiert werden, und verdient mit daran, wenn Sie diese Waren kaufen. Und da er speichern kann, welche Waren Sie kaufen, kann er immer exakter die Waren bestimmen, die Sie kaufen werden. Nur Sie selbst wissen noch gar nicht, dass Sie diese Waren kaufen wollen. Er verfügt also fortan über all Ihre Daten, all Ihre Geheimnisse, und kann damit machen, was er will. Die Dritten, an die er die Informationen weitergeben wird, benennt er nicht genau, sondern nennt sie nur ominös seine „Partner“.

Mal ehrlich: Gäbe es einen solchen Bäcker, würden Sie ihm diese Informationen geben, sein Dokument unterschreiben, seine Brötchen kaufen? Sicherlich nicht. Aber wenn Sie zum Beispiel ein Google-Konto eröffnen, um die verschiedenen Google-Dienste wie Google Calendar, Google Maps oder ähnliches zu verwenden, tun Sie genau dies.

Sie klicken nämlich auf eine Schaltfläche, auf der steht: „Ich akzeptiere die Nutzungsbedingungen“ und wahrscheinlich nehmen Sie sich nicht die Zeit, die seitenlangen Erklärungen zu lesen, die Sie da unterschreiben. Nicht nur das, Sie akzeptieren die Nutzungsbedingungen auch, wenn Sie überhaupt kein Google-Konto eröffnen, sondern einfach nur die Google-Suchmaschine verwenden, denn auch dann stimmen Sie als User diesen Nutzungsbedingungen zu, denn Sie verwenden eine Dienstleistung, die Ihnen Google zur Verfügung stellt.

Der einzige Grund, warum wir alle (oder zumindest die meisten von uns) dies gedankenlos tun, ist: weil es so einfach ist. Dem Bäcker all unsere Geheimnisse persönlich zu erzählen würde sehr lange dauern, in der digitalen Welt werden aber all diese Geheimnisse ohne Mühe gesammelt, gespeichert, archiviert. Und der Speicherplatz ist grenzenlos und wächst schneller als die Datenmengen.

In meinem Stück „Ich akzeptiere die Nutzungsbedingungen“ habe ich daher Auszüge dieser Nutzungsbedingungen vertont – durch die Transformation in Musik wirken manche Satzwendungen ganz anders als beim schnellen Durchlesen. Das ist beabsichtigt. Kein Satz wurde von mir geändert oder hinzugefügt, ich habe den Text nur gekürzt, damit das Stück nicht eine Stunde dauert. Im Stil ist das Stück am ehesten mit einer Kantate zu vergleichen – der Sänger singt jeweils längere zusammenhängende Passagen der Nutzungsbedingungen, ohne diese zu parodieren oder dramatisch aufzuladen. Gerade die Textverständlichkeit war mir hierbei besonders wichtig. Durch die Transformation der trockenen Texte in melodische und durchaus auch emotional aufgeladene Konzertmusik entsteht ein beabsichtigter Verfremdungseffekt, denn normalerweise nimmt man sich ja nicht die Zeit,

diese Art von Texten im Inneren nachklingen zu lassen und über deren tiefere Bedeutung nachzudenken. Hierbei soll die Musik helfen.

Vorgetragen wird das Ganze von einem Bariton, der von einem größeren Streicherensemble begleitet wird (bei der Uraufführung in Frankfurt waren es der Sänger Peter Schöne und das Skyline-Orchester dirigiert von Michael Sanderling).

Fast wäre die Aufführung am [18. Oktober 2014] in der Frankfurter Paulskirche nicht zustande gekommen – die Auftraggeber machten sich, nachdem sie den Titel des Stücks erfahren hatten, große Sorgen, ich hätte hier eine Art SM-Kantate vertont (was angesichts dessen, was Google mit uns macht, vielleicht gar nicht so fern der Wahrheit ist). Dann waren sie aber Feuer und Flamme – der Text der Nutzungsbedingungen wurde sogar ausgelegt und war als „Kleingedrucktes" zu lesen. Soweit ich beurteilen kann, kam die Intention des Stückes bei den Hörern an, auch wenn diese angesichts einer Festveranstaltung mit vielen Reden wahrscheinlich das Allerschlimmste von einem zeitgenössischen Stück über diese Thematik erwartet hatten. Anfängliches Misstrauen kippte um in große Begeisterung. Sogar der anwesende Bundespräsident rutschte zuerst deutlich wahrnehmbar bei den ersten Takten nervös auf seinem Stuhl herum – obwohl ihn die Thematik angesichts seiner persönlichen Vergangenheit sicherlich interessiert haben sollte. Wie er das Stück dann fand, konnte ich ihn nicht mehr fragen, denn er wurde unter seinen eigenen „Nutzungsbedingungen" von einem Pulk von Security-Leuten nach der Veranstaltung aus dem Saal gebracht, während das Publikum die Plätze nicht verlassen durfte.

Hier möchte ich betonen, dass sich mein Stück nicht spezifisch gegen Google wendet. Die meisten Nutzungsbedingungen – zum Beispiel von iTunes, Microsoft, Facebook etc. – ähneln sich im Grunde und sind nur leicht anders formuliert. Manche Passagen sind sogar vollkommen austauschbar und könnten auf viele Internetnutzungen zutreffen.

Ich weiß nicht, ob wir nun alle mehr nachdenken werden, wenn wir das Internet nutzen. Aber ich weiß eines: Wenn wir diesen zunehmenden Verlust von Freiheit und Privatsphäre weiterhin klaglos akzeptieren, wird der Tag kommen, an dem wir zu reinen Arbeits- und Konsumdrohnen verkommen, zu einer Masse von Menschen, die aufs Einfachste manipuliert und unterdrückt werden kann und dabei noch bestens bei Laune gehalten wird. Vielleicht ist das auch längst schon so.

Und ich weiß noch etwas – vielleicht sollten wir nicht alle Kekse (oder „cookies") die uns diese digitalen Bäckergesellen im Internet anbieten, so bedingungslos schlucken. Denn man soll keine Süßigkeiten von Fremden annehmen. Man weiß nie, ob sie es gut mit einem meinen.

Bürgerinitiativen protestieren gegen BND-Etat



Bild: Campact

Am 27.11.2014 um 08:30 Uhr fanden sich bei kaltem Wind Aktive verschiedener Bürgerrechtsorganisationen (Campact, Digitalcourage, FIfF, wastun, DVD, Humanistische Union und Digitale Gesellschaft) vor dem deutschen Bundestag zur Demonstration gegen Steuerverschwendung und Überwachungswahn ein.

Zusammen hatten die Bürgerrechtsorganisationen aufgerufen, gegen das unsinnige Verpulvern von Steuergeldern zu protestieren, kurz vor der Beschlussfassung durch den deutschen Bundestag, dem Bundesnachrichtendienst (BND) zusätzlich zum normalen Budget weitere 300 Millionen Euro bis 2020 zur Verfügung zu stellen. Während der Demonstration wurde von einer Merkel-Darstellerin und einem Gabriel-Darsteller unter lautem Protestlärm den anwesenden Spion-Darstellern mit vollen Händen die 300 Millionen zugeworfen.

Wofür will der BND die zusätzlichen Mittel? Mit dem neuen Haushalt sollen auch neue Gelder für neue Überwachungstechnologien im Rahmen der "Strategischen Initiative Technik" bewilligt werden. Unter anderem sollen von dem Geld exklusive Informationen über Sicherheitslücken in Computersystemen aus zweifelhaften Quellen gekauft werden. Nicht etwa um die Bürgerinnen und Bürger zu schützen, sondern um noch besser digital in Systeme einbrechen zu können.

Den bei der Demonstration anwesenden Politikern der Opposition (Anja Hajduk und Konstantin von Notz von den Grünen, Dietmar Bartsch und André Hahn von der Linken) wurden 142.000 Unterschriften für eine schärfere Kontrolle der Geheimdienste und den Schutz von Hinweisgebern wie Edward Snowden übergeben. Regierungspolitiker blieben trotz mehrfacher Aufforderung der Demonstration fern.

Maut-Pläne sind eine Datenschutz-Zeitbombe

Presseerklärung der DVD e.V. vom 12. November 2014

Die Deutsche Vereinigung für Datenschutz e. V. (DVD) kritisiert den Entwurf eines Gesetzes zur Einführung einer Infrastrukturabgabe für die Benutzung von Bundesfernstraßen. Der Entwurf verstößt gegen wichtige Datenschutzprinzipien. „Warum soll die Maut überhaupt elektronisch kontrolliert werden? Einige unserer Nachbarländer haben zwar ebenfalls Mautsysteme, setzen dabei jedoch auf Papiervignetten und Polizeikontrollen; so spart man sich aufwendige Datenbanken und verzichtet auf ein flächendeckendes Überwachungssystem.“, beanstandet Vorstandsmitglied Reinhard Linz.

Wird jedoch ein automatisiertes Kontrollsystem eingerichtet, müssen die Grundprinzipien des Datenschutzes, insbesondere die Zweckbindung, eingehalten werden. Die DVD moniert insbesondere, dass zu Abrechnungszwecken quasi nebenbei umfangreiche Bewegungsprofile von Autofahrern entstehen werden. Will sich ein Autobesitzer die Maut zurückerstatten lassen, weil er ausschließlich Kreis- und Landstraßen benutzt, soll dies überprüfbar sein. Deshalb sollen Kennzeichen, Fotos sowie Zeit und Ort der Straßennutzung für bis zu 13 Monate gespeichert werden. Hierzu sagt Vorstandsmitglied Frank Spaeing: „Die Kontrolle von Rückzahlungsansprüchen ist doch überflüssig. Für Inländer sollen Maut und Steuersenkung die Gesamtbelastung unverändert lassen: Wer Maut zahlt, dessen KFZ-Steuer wird in gleicher Höhe gesenkt. Wer keine Maut zahlt, bekommt auch keine Steuersenkung. Warum sollte dann jemand eine Rückzahlung der Maut beantragen?“

Große Datensammlungen wecken zudem stets Begehrlichkeiten. Der Präsident des Bundeskriminalamts, Jörg Ziercke, und auch der Berufsverband der Kriminalbeamten haben bereits gefordert, der Polizei Zugriff auf die Bewegungsdaten zu gewähren. Noch steht eine strenge Zweckbindung der Mautdaten im Gesetzentwurf. Aber das kann später durch Gesetzesänderungen aufgeweicht werden. Außerdem fehlen in dem Gesetzesentwurf jegliche Regelungen zur Datensicherheit. Die DVD gibt hierzu zu Bedenken, dass das Bundesverfassungsgericht bereits in seinem Urteil zu Telekommunikations-Vorratsdaten „hinreichend anspruchsvolle und normenklare Regelungen hinsichtlich der Datensicherheit“ gefordert hat. „Hier sehen wir bezüglich des Gesetzesentwurfs großen Nachholbedarf“, betont Vorstandsmitglied Frans Valenta.



Werbung der CSU für die Maut-Pläne.
Quelle: http://www.csu.de/common/_migrated/csucontent/wandzeitung_maut_quer_02.pdf

Aus Sicht der DVD wird mit Einführung der Pkw-Maut erneut eine Infrastruktur geschaffen, welche zur Überwachung der Bürgerinnen und Bürger ausgenutzt werden kann, wenn sich das politische Klima ändert. Wenn nur für eine hohe Kontrolldichte umfangreiche Bewegungsprofile angelegt werden, betrachtet die DVD das als Verstoß gegen den Datenschutzgrundsatz der Erforderlichkeit und Datensparsamkeit. Die DVD fordert daher den Deutschen Bundestag auf, keinem Gesetz zuzustimmen, das unangemessen und zugleich unnötig Bewegungsprofile von Kfz-Nutzern speichert. Für die übrigen Mautdaten muss eine strenge Zweckbindung gelten. Regelungen zur Sicherheit, etwa bei der Datenübermittlung, und zu einer zuverlässigen Datenlöschung zum frühestmöglichen Zeitpunkt müssen außerdem in das Gesetz aufgenommen werden.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

DatenschützerInnen warnen vor PKW-Maut-System

Bundesverkehrsminister Alexander Dobrindt hat am 30.10.2014 sein neues Mautkonzept vorgestellt. Demnach soll es eine Abgabe für Personenkraftwagen (PKW) auf Autobahnen geben. Das Unternehmen Toll Collect kontrolliert bereits, ob die LKW-Maut bezahlt wurde, indem es die Fahrzeuge an Mautbrücken erfasst, die sich über die Fahrbahn spannen. Dobrindt plant ähnliches nun auch für PKW, die er ab 2016 ins Mautsystem einbeziehen will. Über das Kennzeichen soll das Bundesamt für Güterverkehr (BfG) feststellen können, ob die Maut für einen PKW entrichtet ist oder nicht. Dazu gleicht es die Autonummer mit dem sogenannten Infrastrukturabgaberegister ab, in dem das Kraftfahrtbundesamt (KBA) in Flensburg alle MautzahlerInnen erfassen soll. Die Maut soll für alle Autos und Wohnmobile bis 3,5 Tonnen Gewicht auf Autobahnen erhoben werden. Inländische Fahrzeughalter werden unter dem Strich nicht belastet, weil sie die Mautgebühr erstattet bekommen.

DatenschützerInnen fürchten von Anfang an, dass mit dem Mautkontrollsystem Bewegungsprofile von AutofahrerInnen erstellt werden und dass Behörden die Daten auch für andere Zwecke nutzen könnten, als Mautpreller dingfest zu machen. Der rheinland-pfälzische Datenschutzbeauftragte Edgar Wagner meinte: „Besser wäre es, auf Techniken zu verzichten, die solche Gefahren für den Datenschutz hervorrufen.“ Zwar verstoße die Erfassung von Nummernschildern aus Sicht von Bundesverfassungs- und Bundesverwaltungsgericht nicht grundsätzlich gegen den Datenschutz. Allerdings ermögliche das PKW-Mautsystem eine lückenlose Erfassung aller VerkehrsteilnehmerInnen – und eine Löschung der Daten könnte technisch auch einfach unterbleiben.

Die Bundesdatenschutzbeauftragte Andrea Voßhoff kritisierte die Vorschläge nicht grundsätzlich, sondern kündigte an, sie werde „mindestens die hohen datenschutzrechtlichen Standards der Lkw-Maut einfordern“. Das betreffe insbesondere die „strenge Zweckbindung und die Pflicht zur unverzüglichen Löschung“. Grünen-Parteichef Cem Özdemir warnte den CSU-Minister: „Einen gläsernen PKW-Fahrer darf es nicht geben.“ Geht es nach dem Text des inzwischen an die Öffentlichkeit gelangten PKW-Maut-Gesetzes (InfrAG-E), dann wird es diesen gläsernen Autofahrer geben: Als „Kontrolldaten“ sollen gem. § 10 Abs. 2 S. 1 InfrAG-E folgende Daten 13 Monate lang vorgehalten werden: „1. Bild des Kraftfahrzeugs, 2. Name und Anschrift der Person, die das Kraftfahrzeug führt, 3. Ort und Zeit der Benutzung von Straßen im Sinne des § 1 Absatz 1 [Autobahnen und Bundesstraßen], 4. Kennzeichen des Kraftfahrzeugs.“ Zweck dieser Vorratsspeicherung ist, einen Nachweis zu haben, wenn ein deutscher PKW-Nutzer nach einem Jahr behauptet, nie auf einer Autobahn gefahren zu sein und sich deshalb die Maut zurückerstatten lässt (§ 12 Abs. 3 InfrAG-E).

SZ-Kommentator Pascal Paukner meinte, die CDU/CSU-Stammtisch-Parole „freie Fahrt für freie Bürger“ werde durch das vorgestellte Mautkonzept der Bundesregierung in das Gegenteil verkehrt: „Ein Bürger, dessen Nummernschild sprichwörtlich an jeder Straßenecke überwacht wird, kann nicht frei sein. Er ist ein unfreier Bürger.“ Und der Kommentar von Gregor Honsel von Technology Rewiew: „´Surveillance by Design` nennt man so etwas. Da werden – wie bereits bei der LKW-Maut – massenhaft Daten erhoben, die dann wunderbar etwa eine Rasterfahndung ermöglichen. Natürlich werden die Verantwortlichen beteuern, die Daten seien gesichert, werden nur für die angegebenen Zwecke benutzt und schleunigst wieder gelöscht. Jaja, ist klar. Hier tut sich für mich ein Zeitparadoxon auf: Ich kann die Beteuerungen schon nicht mehr hören, obwohl sie noch gar nicht ausgesprochen wurden. Glaubt irgendjemand ernsthaft, der BND oder die NSA kommen an diese Daten nicht ran, wenn sie wirklich wollen?“

Im LKW-Mautgesetz ist festgelegt, dass Toll Collect die erfassten Mautdaten nicht weitergeben darf – auch nicht zur Ermittlung von Schwerverbrechern, wie es Dobrindts Amtsvorgänger Hans-Peter Friedrich vor einiger Zeit angeregt hatte. Das Ministerium spricht von einer „außerordentlich restriktiven Regelung“. Der Gesetzesentwurf für die PKW-Maut sieht vor, dass die an den Straßen erfassten Daten nach der Mautzahlungsprüfung sofort wieder gelöscht werden, sofern die Maut bezahlt ist. Solange das sichergestellt ist, können auch keine Bewegungsprofile von AutofahrerInnen entstehen. Nur wenn jemand die Maut noch nicht bezahlt hat, sollen die Daten vorübergehend im Speicher bleiben und ein Bußgeldbescheid verschickt werden. Dass eine strenge Zweckbindung der Daten auf Widerstand stoßen würde, war absehbar. Als prominentester der vielen Vertretern der Sicherheitsbehörden forderte der Chef des Bundeskriminalamtes Jörg Zierke, die Daten „in besonderen Ausnahmefällen der Schwerstkriminalität“ den Ermittlungsbehörden zur Verfügung zu stellen.

Dobrindt wies die Bedenken der KritikerInnen zurück: „Wir haben die härtestmöglichen Datenschutzregeln in unser Gesetz aufgenommen, die wir in Deutschland kennen.“ Deshalb müsse kein Bürger die Sorge haben, „dass jetzt irgendwo Profile gespeichert werden

könnten“. Im Hinblick auf eine mögliche Doppelnutzung der Daten ergänzte er: „Ich garantiere: Eine Weitergabe an andere Behörden findet nicht statt.“ Der Plan von Dobrindt sieht vor, dass AutofahrerInnen für Fahrzeuge aus dem Ausland online oder an Tankstellen die Maut für ihr Auto entrichten. Dabei geben sie auch das Kennzeichen ihres Autos an. Inländische Fahrzeughalter erhalten per Post jährlich einen Zahlungsbescheid aus Flensburg, der sich nach Hubraum und Schadstoffklasse richtet. Zugleich senkt die Finanzbehörde die Kfz-Steuer um den entsprechenden Betrag, sodass deutsche Autofahrer nicht mehr zahlen müssen – ein Versprechen der Union aus dem Koalitionsvertrag. Vignetten zu kleben soll nicht notwendig sein (Stratenschulte/dpa, Datenschützer warnen vor Zweckentfremdung des Maut-Systems, www.zeit.de 31.10.2014, Paukner, Freie Fahrt für unfreie Bürger, www.sueddeutsche.de 31.10.2014; Bergt, Das Maut-Gesetz analysiert: 13 Monate Vorratsspeicherung auf den Straßen, www.cr-online.de 01.11.2013; Sauerbrey, Daten können bis zu 13 Monate lang gespeichert werden, www.tagesspiegel.de 02.11.2014).

Bund

BDSG-Änderung zur Organisation der BfDI

Mit einem vom Bundeskabinett am 27.08.2014 beschlossenen Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes (BDSG) soll die verfassungsrechtlich und europarechtlich geforderte völlige Unabhängigkeit des Amtes der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) hergestellt werden (BR-Drs. 395/14). Bundesinnenminister Thomas de Maizière hatte diese Initiative schon bei der Amtseinführung der neuen BfDI Andrea Voßhoff im Februar 2014 angekündigt. Der Europäische Gerichtshof hatte mit seinen Entscheidungen zur deutschen Datenschutzaufsicht (09.03.2010) und zur österreichischen Datenschutzkommission (16.10.2012) festgestellt, dass eine Rechts- und eine Dienstaufsicht mit der Unabhängigkeit der Datenschutzkontrolle nicht vereinbar sind. Sämtliche Bundesländer haben aus dieser Rechtsprechung ihre Konsequenzen gezogen. Der Bund wurde erst aktiv, nachdem die Europäische Kommission mit einem weiteren Verfahren gegen Deutschland drohte.

Ein vorrangiges Anliegen des Entwurfes ist es, der Realität hinterherhinkend, klarzustellen, dass auch Frauen BfDI sein können. Es wird eine oberste Bundesbehörde geschaffen, die nicht mehr in das Bundesinnenministerium (BMI) eingebunden ist, das nicht nur für den Datenschutz, sondern vor allem für die Sicherheitsbehörden zuständig ist. Während in den Bundesländern regelmäßig das Vorschlagsrecht den demokratisch legitimierteren und weniger von Eigeninteressen geleiteten Parlamenten zugewiesen ist, soll dies im Bund nach dem Willen der Regierung bei ihr verbleiben. Bei Zeugenaussagen der BfDI, die den “Kernbereich exekutiver Eigenverantwortung der Bundesregierung” möglicherweise betreffen, muss “Einvernehmen mit der Bundesregierung” hergestellt werden. Es ist ungewöhnlich, dass eine kontrollierte Regierung zustimmen muss, wenn zwei Kontrollinstanzen, also etwa die BfDI und ein Bundestags-Untersuchungsausschuss oder ein Gericht, sich austauschen wollen. In dem Gesetzentwurf heißt es: “Zugleich wird die Datenschutzaufsicht auf Bundesebene insgesamt gestärkt.” Tatsächlich wird die Besoldung der BfDI angehoben. Vorgesehen sind zudem vier neue Stellen, die aber wohl für die neuen personal- und haushaltswirtschaftlichen Aufgaben der Dienststelle benötigt werden dürften.

In der europäischen Datenschutzrichtlinie ist verpflichtend vorgesehen, der Datenschutzkontrolle “wirksame Eingriffsbefugnisse” zu übertragen, die beispielhaft genannt werden: “geeignete Veröffentlichung (von) Stellungnahmen, […] die Befugnis Sperrung, Löschung oder Vernichtung von Daten oder […] das Verbot einer Verarbeitung anzuordnen”. In den Entwürfen für eine EU-Datenschutz-Grundverordnung sind als wirksame Sanktionsmöglichkeiten Bußgelder in Höhe von zwei bis fünf Prozent des Unternehmensumsatzes geplant. Dem gegenüber soll der BfDI lediglich die Möglichkeit einer “Beanstandung” zur Herbeiführung rechtskonformer Zustände bleiben, selbst bei den Post- und Telekommunikationsunternehmen. Das Äußerungsrecht der BfDI, bisher eine wirksame Waffe der Datenschutzbeauftragten, wird im Widerspruch zum Geist der europäischen Regelung nicht gestärkt.

Der vorherige BfDI Peter Schaar bezeichnete den Gesetzentwurf als „völlig unterambitioniert“ und äußerte die Hoffnung, dass substanziell nachgebessert wird: „Allerdings bin ich skeptisch, ob dies angesichts der überwältigen Mehrheit der Regierungsparteien geschehen wird“. Druck von der Amtsinhaberin ist nicht zu erwarten, die keine inhaltliche Kritik an den Vorschlägen äußerte, sondern nur meinte: „Ich würde mich freuen, wenn der Gesetzgeber meine Vorschläge für eine angemessene haushaltsmäßige Ausstattung meiner Dienststelle in einem breiten Konsens konstruktiv aufgreift.“ Man könnte den Eindruck haben, dass sich die BfDI ihre Willfährigkeit durch Stellen bezahlen lassen möchte. Eine Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08.10.2014 kritisiert zusätzlich, wenn auch verhalten, die Regelungsvorschläge und appelliert an den Bundesgesetzgeber, der BfDI effektive Sanktionsmittel an die Hand zu geben (Schaar, Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes „völlig unzureichend“, www.netzpolitik.org 27.08.2014; Voßhoff, PM 16.10.2014, Nur eine funktionsfähige Datenschutzbehörde ist auch unabhängig).

Bund

BND-Datenschutzbeauftragte berichtet im NSA-Ausschuss

Vor dem NSA-Untersuchungsausschuss berichtet die Datenschutzbeauftragte des Bundesnachrichtendienstes (BND), Frau F., am 09.10.2014 von ihren Erfahrungen im deutschen Auslandsgeheimdienst. Die Volljuristin ist seit neun Jahren für den BND tätig, seit zweieinhalb Jahren ist sie dort Datenschutzbeauftragte und damit direkt dem Präsidenten Gerhard Schindler in Ber-

lin unterstellt. Persönliches, auch ihren vollen Namen, durften die Abgeordneten des NSA-Ausschusses gemäß den Vorgaben ihres Arbeitgebers nicht von Frau F. erfahren. Die Aussage der Geheimdienstmitarbeiterin vor dem parlamentarischen Untersuchungsgremium ist aber interessant, weil sie offenbart, wie wenig ernst der BND viele Jahre lang das Thema Datenschutz – bis heute – nahm bzw. nimmt.

Als Frau F. 2012 Datenschutzbeauftragte des BND wurde, war die Abteilung bereits lange führungslos gewesen. Sie selbst sei „technisch nicht vorgebildet“, habe nur juristisches Wissen mitgebracht. Im Umgang mit den vielen Daten, die der Auslandsgeheimdienst so sammle, müsse sie sich auf die technische Expertise der KollegInnen im Dienst verlassen. In der Regel lasse sie sich die Datenbank vorführen und stelle Fragen dazu. Ob hier eine wirkliche Kontrolle stattfinden kann, sei dahin gestellt. Für viele brisante Themen sei sie als Datenschutzbeauftragte überhaupt nicht zuständig. So kümmert sich ein eigener Hausjurist um alle Daten, die die nach Art. 10 Grundgesetz (GG) geschützte Telekommunikation zwischen Deutschen betreffen und um die rechtlich heiklen Fragen rund um deren Auswertung, Speicherung und Weitergabe nach dem G10-Gesetz.

Zu vielen Geheimdienstaktivitäten, die den NSA-Ausschuss interessieren, konnte Frau F. nichts sagen: Von den angezapften Glasfaserkabeln hat sie angeblich nur in der Zeitung gelesen, über den Umgang mit Kommunikationsdaten am Knotenpunkt Frankfurt und den Fall Eikonal konnte sie auch nichts berichten. Letzterer habe sich ja wohl vor ihrer Zeit zugetragen. „Bestimmte Bereiche der Informationserfassung werden Ihnen vorenthalten“, fasst die Obfrau der Linken, Martina Renner, die Situation zusammen. Der für die brisanten Dinge zuständige G10-Jurist im BND ist nicht weisungsunabhängig wie die Datenschutzbeauftragte. Der Mann wurde im Ausschuss nach Frau F. in nicht öffentlicher Sitzung angehört.

Die Datenschutzbeauftragte berichtete freimütig über einen Streit mit ihrem Chef, BND-Präsident Schindler, zum BND-Standort Bad Aibling, an dem die deutschen Geheimdienstler Satellitendaten aus dem Ausland erfassen und auswerten, etwa Telefongespräche in Afghanistan und Pakistan. Auf dem Gelände in Bad Aibling sind auch Mitarbeiter des amerikanischen Geheimdienstes NSA stationiert. Schindler wähnt die Satellitendaten des BND nach Schilderung von F. im weitgehend rechtsfreien Raum – denn sie seien ja im Weltall erhoben, in dem keine deutschen Gesetze griffen, so dass auch § 19 BVerfSchG nicht anwendbar sei. Dem setzte F. entgegen: „Meiner Meinung nach werden die Daten in Bad-Aibling erfasst und damit im Geltungsbereich des BND-Gesetzes.“ Daher müssten ihrer Meinung nach auch für afghanische Telefongespräche die strengeren deutschen Daten- und Kommunikationsschutzbestimmungen gelten. Das bedeute, dass die geheimdienstlich ermittelten Daten von AusländerInnen nicht so einfach an „ausländische Stellen“ weitergegeben werden könnten. Den von der Überwachung Betroffenen müsse der BND die Übermittlung mitteilen, „sobald eine Gefährdung seiner Aufgabenerfüllung durch die Mitteilung nicht mehr zu besorgen ist“ Außerdem wies Frau F. darauf hin: „Laut BND-Gesetz hat eine Übermittlung zu unterbleiben, wenn auswärtige Belange der BRD oder schutzwürdige Interessen betroffen sind.“

Der SPD-Obmann im Ausschuss, Christian Flisek, fasste die Aussage von Frau F. dahingehend zusammen, dass die BND-Leitung sich die Weitergabe der Ausland-Ausland-Kommunikation an andere Dienste offenbar so einfach wie möglich machen wolle. Schon zu Beginn des NSA-Ausschusses hatten Verfassungsrechtler Bedenken angemeldet, was die rechtliche Grundlage für die Behandlung der abgefangenen Satellitendaten in Bad Aibling betraf. Die Datenschutzbeauftragte berichtete dem Ausschuss von einer „intensiven rechtlichen Diskussion“ auf Leitungsebene des BND, bei der sie „leider überstimmt worden“ sei. Sie habe eben nur eine „Beratungsfunktion“ inne. F. geht aber davon aus, dass der BND sich auch ohne eine gesetzliche Einschränkung beim Umgang mit Daten, z. B. aus afghanischen Telefongesprächen, an „bestimmte Standards“ halte. Diese seien „Schutz der Menschenwürde, Willkürverbot und Verhältnismäßigkeit“.

Frau F. betreut nach eigener Angabe beim BND rund 25 Datenbanken mit Geheimdienstinformationen. Ihre Aufgabe sei es, sicherzustellen, dass sie den Datenschutzgesetzen entsprechen. Es werde derzeit versucht, kleinere Datenbanken zu größeren zusammenzufügen. Zudem benutzt der deutsche Geheimdienst rund 20 Tools der NSA, darunter das Programm XKeyscore. Details zu den Funktionen der Tools wollte F. jedoch nur in nichtöffentlicher Sitzung erläutern. Auch zu den BND-Programmen gab F. wenig Details preis. Sie räumte allerdings ein, dass das Programm Veras die Metadaten von Verdächtigen bis in die vierte und fünfte Ebene abspeichere.

Vor allem in der BND-Abteilung Technische Aufklärung seien ihr Mängel aufgefallen. So seien bei ihrem Amtsantritt zwei Datenbanken mit Personendaten nicht, wie rechtlich vorgesehen, vom damaligen Bundesdatenschutzbeauftragten (BfDI) geprüft und dann vom Kanzleramt genehmigt worden – und das obwohl sie seit Jahren in Betrieb seien. Eine davon sei die seit 2001 genutzte Datenbank INBE, die Informationen über deutsche Staatsbürger enthalte, ohne dass ein vorgeschriebenes Dateianordnungsverfahren durchgeführt worden sei: „Man speicherte so lange, bis der Speicher volllief.“ Glücklicherweise habe dies meistens nur zwölf Monate lang funktioniert; der Gesetzgeber erlaube bis zu 24 Monate Speicherfrist. Bei der Datenprotokollierung habe es Mängel gegeben. Frau F. erklärte die Versäumnisse mit einer möglichen Unkenntnis der Mitarbeitenden, die sie mit einem umfangreichen Schulungsprogramm beheben will.

Diskussionen führe die Datenschutzbeauftragte noch mit der Abteilung Technische Aufklärung und der neuen BfDI über die 2010 eingerichtete Datenbank VERAS, in der zum Großteil Verbindungen zwischen ausländischen Personen erfasst würden: „Mit wem hat Terrorist X telefoniert in den letzten zwei Wochen?“ Auch hier fehlt es an der nach § 14 BVerfSchG geforderten Dateianordnung, die der Zustimmung des Bundeskanzleramts bedarf. Frau F. befürchtet, dass hier eine anlasslose Vorratsdatenspeicherung durchgeführt werde; das sei nicht vereinbar mit deutschen Gesetzen. Die Mängel seien ihr im Jahr

2013 erst anlässlich interner Mitarbeiterschulungen aufgefallen. Damit sei die Nutzung der Datenbanken formell, nicht aber materiell rechtswidrig (Caspari, Der BND pfeift auf seine Datenschutzbeauftragte, www.zeit.de 09.10.2014; BND-Datenschutzbeauftragte: BND versäumte Datenschutzprüfung bei Datenbanken, www.golem.de 09.10.2014).

Bund

Deutsche BKK gibt Daten an Schufa

Die Deutsche Betriebskrankenkasse (BKK) hat sich bei der Schufa nach der finanziellen Lage Tausender Schuldner erkundigt. Seit März 2011 haben Mitarbeitende der Abteilung Vollstreckung/Insolvenz der Deutschen BKK in bis zu 11.000 Fällen eine Auskunft bei der Schufa eingeholt. Die Deutsche BKK, eine gesetzliche Kasse mit 800.000 Versicherten, konsultiert die Schufa etwa, wenn freiwillig Versicherte, z. B. Selbstständige oder Arbeitgeber, ihre Beiträge nicht gezahlt haben. Das Verfahren trage, so eine Sprecherin, dazu bei, „wirtschaftlich unnötige Vollstreckungshandlungen zu vermeiden." Der damalige Bundesdatenschutzbeauftragte Peter Schaar hatte schon 2009 in einem anderen Fall Zweifel an Ablauf und Notwendigkeit eines solchen Austausches angemeldet, da die Schufa-Anfrage nicht ohne die Übermittlung von Sozialdaten möglich ist. Eine derartige Übermittlung von Sozialdaten, wozu auch Namen oder Geburtsdaten von Versicherten gehören, ist Krankenkassen nach dem Sozialgesetzbuch (SGB) verboten. Die Deutsche BKK bestreitet, dies im Rahmen des Vertrags mit der Schufa zu tun und wird von dieser unterstützt: „Die Schufa hilft Forderungen von Personen einzubringen, die trotz mehrfacher Aufforderung fällige Versicherungsbeiträge schuldig geblieben sind. Die Datenübermittlung ist gesetzlich zulässig und liegt auch im Interesse der Gesellschaft und der Versicherten." Man zähle zudem nur einige wenige gesetzliche Kassen zu seinen Kunden. Das Bundesversicherungsamt will als Aufsichtsbehörde den Vorgang erneut prüfen (Hunger auf Daten, Der Spiegel 36/2014, 60 = Deutsche BKK fragt Daten von Schuldnern bei der Schufa ab, www.spiegel.de 31.08.2014).

Bund

„Pay as you drive" bei Signal Iduna

Die Signal Iduna stellte ein Kfz-Versicherungspaket für junge Erwachsene vor, bei dem die Höhe der Beiträge vom Fahrstil abhängig gemacht wird. Ein Dongle, der an die Diagnoseschnittstelle (OBD2) des Autos gesteckt wird, meldet Fahrzeugdaten per Bluetooth an eine Smartphone-App, die den Fahrstil analysiert und dabei Beschleunigung, Kurvengeschwindigkeit und Bremsverhalten berücksichtigt. Daraus wird ein individueller Score berechnet, an dem sich die Beitragshöhe bemisst. Anders als beim umstrittenen Telematik-Angebot der Sparkassen-Direktversicherung werden keine GPS-Daten erfasst.

Die Versicherung bietet den sogenannten AppDrive-Tarif über ihre Marke sijox an. Er richtet sich an Fahrer unter 30 Jahren und gilt nur für das Paket „Meine Mobilität", das außer der Kfz- auch eine Unfall- und Verkehrsrechtsschutz-Versicherung enthält. AppDrive startet mit einer Beitragsermäßigung von 15%; durch umsichtiges Fahren soll eine weitere Senkung um 25% möglich sein. Nachforderungen, wenn sich der Fahrstil ändert, schließt die Versicherung aus.

Die FahrerIn kann ihren AppDrive-Score am Handy auslesen und erhält Tipps, wie sich dieser verbessern lässt. Die App gibt es für Android und iOS. Sie zeigt auch an, wie viel man aktuell spart. Als OBD2-Dongle nutzt Signal Iduna den TomTom Link 100. Er soll Versicherungen, Fahrzeugherstellern, Pannendiensten und Leasingunternehmen den einfachen Zugriff auf Daten zum Fahrverhalten und zur Fahrzeugnutzung ermöglichen. TomTom betont, dass Bedenken hinsichtlich des Datenschutzes überflüssig seien, da keine GPS-Daten erfasst werden. Allerdings speichert der Link 100 Daten zwischen, die z. B. auch nach einem Unfall ausgewertet werden könnten, um die Schuldfrage zu klären (Signal Iduna analysiert Fahrstil für individuelle Kfz-Versicherung, www.heise.de 30.10.2014).

Bund

Google bietet Arztsprechstunde per Videochat

Der Internetkonzern Google testet einen Dienst, bei dem Nutzende per Internet direkt mit ÄrztInnen reden können. Der Digitalkonzern will sie so davon abhalten, sich selbst zu diagnostizieren. Wenn eine NutzerIn in die Suchmaske von Reddit eingibt, dass sie Knieschmerzen hat, liefert Google ihr nicht nur Ergebnisse, sondern auch eine kleine Info-Box mit dem Zusatz: „Sprechen Sie jetzt mit einem Arzt." Dies ist nicht als Aufforderung, sondern als Angebot gemeint. Ein Arzt könne per Knopfdruck für einen Videochat dazugeschaltet werden. Geplant ist ein Service im Stil von Google Helpouts, womit Google seit einem Jahr Tipps von ExpertInnen per Videochat anbietet. Helpouts hat momentan acht Kategorien. Wer sich in Sachen „gesundes Essen" beraten lassen will, muss aktuell 15 Dollar pro Stunde zahlen. Wie der Ärzte-Dienst konkret funktionieren wird, ist noch unklar. Dem Screenshot der Reddit-NutzerIn zufolge ist die Beratung während der Testphase kostenlos.

Google versteht sein Angebot als Maßnahme gegen Cyberchondrie, die Online-Variante der Hypochondrie, bei der Menschen im Internet ihre Symptome eingeben, um herauszufinden, woran sie erkrankt sein könnten – und sich selbst diagnostizieren. Laut einer Studie kann diese Suche bei einigen Menschen dazu führen, dass sich die Angstzustände verschlimmern. Ob ein solcher Dienst in Deutschland zulässig wäre, ist fraglich: Laut der Berufsordnung ist es Ärzten untersagt, eine Behandlung „ausschließlich über Print- und Kommunikationsmedien" durchzuführen. Heinrich Körtke, Leiter des westdeutschen Zentrums für angewandte Telemedizin: „Mal angenommen, Sie klagen über Magenschmerzen, und Dr. Google sagt, alles sei in Ordnung. Aber 24 später fallen Sie tot um, weil die Magen-Darm-Blutung nicht erkannt wurde – da kann man Schlimmmes anrichten: Dr. Google beruhigt den Patienten, aber er heilt ihn nicht. Wir brauchen Ärzte und keine Firma, die ausschließlich das Geld

sieht“ (Google schickt den Arzt, www.sueddeutsche.de 13.10.2014; Kann Google uns gesund machen, Herr Körtke? Der Spiegel 43/2014).

Baden-Württemberg

Jahrzehntelange Verfassungsschutzbeobachtung von Anwalt

Rechtsanwalt Michael Moos ist seit über 40 Jahren eine politische Institution in Freiburg. Auch schon seit vielen Jahren ist er für die Linke Liste im Stadtrat der Universitätsstadt. Im Jahr 2009 teilte der Verfassungsschutzbericht, also die jährliche Aufzählung der vom Landesamt für Verfassungsschutz (LfV) als verfassungsfeindlich eingestuften politischen Bestrebungen, mit, dass die Linke Liste unter Beobachtung stehe. Dass der 67jährige Moos als überzeugter Linker politische Gegner hat, ist unvermeidlich; keiner von diesen würde aber wohl dessen persönliche und moralische Integrität in Frage stellen. Er engagierte sich in der 68er Zeit beim Kommunistischen Bund Westdeutschands. In den 70er Jahren vertrat er als Anwalt Klienten, die der RAF-Nähe verdächtigt wurden. Bis heute blieb er politisch aktiv.

Nach der Veröffentlichung im Verfassungsschutzbericht forderte der Anwalt vom LfV Auskunft zu seiner Person. Erst mit Hilfe des Verwaltungsgerichts (VG) Stuttgart konnte dies verbindlich zu einer Auskunft verpflichtet werden. Doch statt der Akten erhielt Moos im Sommer 2013 von Innenministerium in Stuttgart einen Sperrvermerk mitgeteilt, ohne dass dieses offensichtlich die für sperrwürdig erklärte Akte vollständig vorliegen hatte. Wegen dieses Formfehlers musste erneut das VG Stuttgart angerufen werden. Das verfügte, dass der Sperrvermerk erneut geprüft werden muss. Nach weiteren vielen Monaten erhielten das Gericht und hierüber auch Moos ein ca. 700 Seiten starkes Paket Papier, dessen Texte zum größten Teil geschwärzt und damit nicht lesbar sind. Mitgeliefert wurde eine neue 106 Seiten lange Begründung, weshalb die Schwärzungen zur Vermeidung von „Nachteilen für das Wohl des Landes“ nötig seien, dass „ihrem Wesen nach geheime Vorgänge“ geheim gehalten werden müssten und „namentliche Hinweise auf Bearbeiter“ unsichtbar zu machen seien.

Erkennbar blieb, dass Moos zumindest seit Ende der 70er Jahre überwacht wurde, wahrscheinlich jedoch schon länger. Einige Male tauchen im Meer der Druckerschwärze die Wörter „linksextremistischer Terrorismus“ auf. Andere ungeschwärzte Sätze klingen banal bis komisch. So vermeldete der Mitarbeiter des Verfassungsschutzes über die „Knete-Fete“ am 21.05.1982: „Getragen wurde der Abend von der Hardrockband ´Die Bremser`“. Weshalb die Beobachtung erfolgte, ist wegen Schwärzungen nicht erkennbar. Zum Schluss heißt es dann: „Das Fest verlief ohne nennenswerte Ereignisse“. Moos kann sich heute an diese Fete nicht mehr erinnern. Ein anderer Auszug: „16.08 Uhr: Moos kommt mit dem Fahrrad aus Richtung Rosastraße zum Objekt. Er stellt das Rad ab und betritt die Kanzlei. ... 17.57 Uhr: Moos verlässt die Kanzlei und fährt weg.“ Das LfV erklärt: „Gerade Verfassungsfeinde arbeiten konspirativ und versuchen, ihre wahren Ziele zu verschleiern. In solchen Fällen darf der Verfassungsschutz unter engen gesetzlichen Voraussetzungen auch nachrichtendienstliche Mittel einsetzen. Dazu gehören insbesondere das Anwerben und Führen von Vertrauensleuten und die Observation verdächtiger Personen. Aus den ungeschwärzten Teilen der Akte geht hervor, dass ein der RAF-Szene zugerechneter Gefangener in Suttgart-Stammheim ebenso überwacht wurde wie sein Verteidiger Michael Moos. Ob die Verteidigergespräche zwischen diesen beiden „Verfassungsfeinden“ belauscht wurden, ergibt sich aus den lesbaren Aktenteilen nicht. Der Anwalt von Moos, Udo Kauß, will am Ende erreichen, dass die Überwachung rechtswidrig war. Um hier hinzukommen, soll nun ein In-Camera-Verfahren angestrengt werden, bei dem sich Richter des Verwaltungsgerichtshofes die ungeschwärzte Akte betrachten, um dann zu entscheiden, ob die Vergangenheit von Moos geschwärzt bleiben muss oder nicht (Kizler, Der Sonntag 08.06.2014).

Hamburg

HmbBfDI erlässt Anordnung gegen Google

Der Hamburgische Beauftrage für Datenschutz und Informationsfreiheit (HmbBfDI) hat Ende September 2014 gegenüber der Google Inc. zur Beseitigung von Verstößen gegen das Telemediengesetz und das Bundesdatenschutzgesetz eine Verwaltungsanordnung erlassen und dabei das US-Unternehmen verpflichtet, Daten, die bei Nutzung unterschiedlicher Google-Dienste anfallen, nur unter Beachtung der gesetzlichen Vorgaben zu erheben und zu kombinieren. Nach Auffassung der für Google in Deutschland zuständigen Datenschutzbehörde greift die bisherige Praxis der Erstellung von Nutzerprofilen weit über das zulässige Maß hinaus in die Privatsphäre der Google-Nutzenden ein. Google wird verpflichtet, technische und organisatorische Maßnahmen zu ergreifen, die sicherstellen, dass deren Nutzende künftig selbst über die Verwendung der eigenen Daten zur Profilerstellung entscheiden können.

Die Google Inc. erhält umfängliche Informationen über die Nutzungsgewohnheiten ihrer KundInnen. Viele setzen die unterschiedlichen vom Unternehmen angebotenen Dienste in ihrem täglichen Leben regelmäßig und umfassend ein. Dies betrifft sowohl die bei Google registrierten Personen, z. B. Gmail-User und die meisten Besitzenden eines Android-Smartphones, als auch Personen, die Google-Dienste, z. B. die Suchmaschine, verwenden. Die Inhalts- und Nutzungsdaten, die dabei anfallen, verraten viel über die einzelne Person und deren Interessen, Gewohnheiten und Lebensweise. Es können damit detaillierte Bewegungsmuster durch Standortdaten erstellt, Rückschlüsse auf spezifische Interessen und Vorlieben durch Auswertung der Nutzung der Google-Suchmaschine gezogen, der soziale und der finanzielle Status, der Aufenthaltsort und viele weitere Gewohnheiten ermittelt und etwa Freundschaftsbeziehungen, sexuelle Orientierung sowie der Beziehungsstatus abgeleitet werden.

In den Privatsphäre-Bestimmungen schließt Google die Verknüpfung be-

sonders sensibler personenbezogener Daten lediglich zu Werbezwecken aus. Nichtsdestotrotz kann die Verknüpfung all dieser Informationen aus den verschiedenen Einzeldiensten aussagekräftige und nahezu umfassende Persönlichkeitsbilder entstehen lassen. Die Bildung solcher diensteübergreifender Profile behält sich Google durch die seit März 2012 geltenden Privatsphäre-Bestimmungen ausdrücklich vor. Da für eine derartig massive Profilbildung unter Zusammenführung aller Daten weder im nationalen noch im europäischen Recht eine Rechtsgrundlage existiert, ist dies nur dann zulässig, wenn der Nutzer ausdrücklich und informiert in eine derartige Verarbeitung seiner Daten eingewilligt hat oder – soweit dies gesetzlich vorgesehen ist – er dagegen widersprechen kann.

Der HmbBfDI Johannes Caspar erläutert: „Zwar konnten wir in zahlreichen Gesprächen mit Google Verbesserungen insbesondere bei der Information der Nutzer erreichen. Bei der wesentlichen Frage der Zusammenführung der Nutzerdaten war Google jedoch nicht bereit, die rechtlich erforderlichen Maßnahmen einzuhalten und substantielle Verbesserungen zugunsten der Nutzerkontrolle umzusetzen. Insoweit wird Google nun per Anordnung dazu verpflichtet. Unsere Anforderungen zielen auf einen fairen, gesetzlich vorgesehenen Ausgleich zwischen den Interessen des Unternehmens und denen seiner Nutzer. Der Ball liegt nun im Spielfeld von Google. Das Unternehmen muss die Daten von Millionen von Nutzern so behandeln, dass deren Recht auf informationelle Selbstbestimmung künftig bei der Nutzung der unterschiedlichen Dienste des Unternehmens hinreichend gewahrt wird.“

Der HmbBfDI ist der Vertreter Deutschlands in einer europäischen Task Force von Datensschutzbehörden, welche die Privatsphäre-Bestimmungen Googles prüft und bewertet. Dabei wurden die inhaltlichen Kriterien zwischen den darin vertretenen sechs EU-Mitgliedstaaten intensiv diskutiert, um eine möglichst einheitliche europäische Sichtweise zu gewährleisten. Die konkrete Durchsetzung der datenschutzrechtlichen Anforderungen erfolgt jedoch unabhängig und allein auf Grundlage des jeweiligen nationalen Rechts. Während zum Teil andere Länder aufgrund ihrer nationalen Bestimmungen Verstöße mit Bußgeldern sanktionierten (Frankreich – DANA 1/2014, 33, Niederlande – DANA 1/2014, 34), wurde nach deutschem Datenschutzrecht nun eine Verwaltungsanordnung erlassen (PM HmbBfDI 30.09.2014, Wesentliche Änderungen bei der Datenverarbeitung von Google notwendig – Datenschutzaufsicht erlässt Anordnung).

Hessen

Schwarz-Grün will Verfassungsschutz neu ordnen

Als Konsequenz aus der NSU-Mordserie soll das Landesamt für Verfassungsschutz (LfV) in Hessen reformiert werden. Die Regierungsfraktionen CDU und Grüne sowie Innenminister Peter Beuth (CDU) stellten in Wiesbaden dazu am 09.10.2014 einen Gesetzesvorschlag bzw. ein Eckpunktepapier vor. Danach soll der LfV zu einer modernen und möglichst transparenten Behörde umgebaut werden, die nicht länger abgeschottet und geheimniskrämerisch wirkt. Als Vorbild wird das Bundesamt für Verfassungsschutz (BfV) genannt. In dem Eckpunktepapier heißt es, das LfV „tauscht sich mit Wissenschaft und Gesellschaft aus. Dazu gehört auch der öffentliche Diskurs.“ Das LfV soll verpflichtet werden, sich mit anderen Landesämtern und dem BfV im Kampf gegen gewalttätigen Extremismus auszutauschen. Defizite in diesem Bereich trugen nach Ansicht von Sicherheitsexperten dazu bei, dass der NSU jahrelang unentdeckt in ganz Deutschland morden konnte. Dem LfV soll es erschwert werden, Informationen über gefährliche extremistische Bestrebungen vor anderen staatlichen Behörden geheim zu halten. Allenfalls bei Gefahr für Leib und Leben von Personen, etwa Informanten des LfV in der Szene, sog. V-Leuten, sind Übermittlungsverbote an andere Sicherheitsbehörden denkbar. Diese sollen aber schriftlich begründet und dem Landesinnenminister sowie dem Parlamentarischen Kontrollgremium des Landtags vorgelegt werden, das das LfV überwacht. Erstmals soll in Hessen klar geregelt werden, dass V-Leute keine schweren Straftaten begehen dürfen. Als Informant sollen sie aber Ordnungswidrigkeiten und kleinere Straftaten begehen dürfen, die in der Szene üblich sind.

Auch die parlamentarische Aufsicht über das LfV soll neu geregelt werden. Vorgesehen ist eine Stärkung des Parlamentarischen Kontrollgremiums. Das Gremium soll in den meisten Fällen zur Verschwiegenheit verpflichtet sein, mindestens zweimal im Lauf der fünfjährigen Legislaturperiode den Landtag über die Kontrollarbeit informieren und darstellen, ob die Landesregierung ihren Verpflichtungen nachkommt, das Gremium über besondere Vorkommnisse zu informieren.

Als die wesentlichen Eckpunkte der Vorschläge werden genannt:

- die gesetzliche Formulierung eines Leitbilds für den Verfassungsschutz,
- die ausdrückliche Normierung des Präventionsauftrags des LfV,
- das Unterstreichen der Zusammenarbeit des LfV mit anderen Behörden,
- eine klare Gliederung der Befugnisse des LfV,
- die ausdrückliche Auflistung der möglichen nachrichtendienstlichen Mittel,
- die gesetzliche Normierung des V-Leute-Einsatzes,
- die klare und vereinfachte Strukturierung der Vorschriften zur Speicherung und Löschung von Erkenntnissen des Verfassungsschutzes und
- die Vereinfachung der Vorschriften zur Informationsübermittlung an andere Behörden.

Die Vorschläge sollen zunächst nicht in den Landtag eingebracht, sondern von einer Expertenkommission unter der Leitung des ehemaligen Richters des Bundesverfassungsgerichts, Prof. Dr. Hans-Joachim Jentsch, begutachtet werden. Diese von Schwarz-Grün berufene Kommission arbeitet parallel an Vorschlägen, wie die Zusammenarbeit der Sicherheitsbehörden in Hessen verbessert werden kann. Man wolle den Ergebnissen des Gremiums, so Vertreter von CDU und Grünen, nicht vorgreifen. Der NSU-Untersuchungsausschuss im Bundestag hat empfohlen, dass der Verfassungsschutz seine Informanten, die V-Leute, stärker kontrolliert. Die

Sicherheitsbehörden sollen sich mehr austauschen (Höll SZ 11./12.10.2014, 7; Hessisches Ministerium des Innern, PM v. 10.10.2014, Innenminister stellt Gesetzentwürfe zur Neuausrichtung des Verfassungsschutzes vor – Expertenkommission wird sich damit kritisch auseinandersetzen).

Mecklenburg-Vorpommern

Land verzichtet auf soziale Medien

Die Regierung des Bundeslandes Mecklenburg-Vorpommern verzichtet künftig auf Auftritte in sozialen Medien wie Facebook und Twitter. Sie sieht in diesen Plattformen keinen größeren Nutzen, der den Einsatz des dafür erforderlichen Personals rechtfertigen würde. Regierungssprecher Andreas Timm: „Wir informieren über Pressemitteilungen und auf unseren Homepages und sehen in den sozialen Netzwerken keinen größeren zusätzlichen Nutzen für uns." Der Landesbeauftragte für Datenschutz und Informationsfreiheit Reinhard Dankert begrüßte diese Trendwende: „Nicht nur die Landesregierung sondern alle öffentlichen Stellen sollten sich ihrer Vorbildwirkung bewusst sein und nicht dazu verleiten, datenschutzrechtlich fragwürdige Angebote zu nutzen." Bereits im Oktober 2011 hatte Dankert alle öffentlichen Stellen des Landes aufgefordert, auf die Nutzung sozialer Netzwerke zu verzichten, weil diese Plattformen nicht mit deutschen und europäischen Datenschutzstandards in Einklang stehen. Über soziale Netze wird unter anderem im Zusammenhang mit dort platzierten öffentlichen Fahndungen der Polizei diskutiert.

Medienwissenschaftler der Technischen Universität Berlin haben hierzu ein Gutachten erstellt, das die Risiken dieser Fahndungsmethode beleuchtet, das am 21.10.2014 ausführlich vorgestellt wurde. Dankert: „Ich begrüße, dass sich auch die Wissenschaft dieses Themas annimmt und die Risiken derNutzung sozialer Netze verdeutlicht" (LfDI Mecklenburg-Vorpommern, PE 14.10.2014, Landesregierung verzichtet auf Nutzung sozialer Medien; Datenschützer begeistert, www.welt.de 14.10.2014).

Niedersachsen

Polizei veröffentlicht Videoüberwachungs-Kataster

Die sechs Polizeidirektionen in Niedersachsen (Braunschweig, Göttingen, Hannover, Lüneburg, Oldenburg, Osnabrück) betreiben in ihren jeweiligen Zuständigkeiten Videoüberwachungsanlagen mit der Zielrichtung der Gefahrenabwehr. Um insofern mehr Transparenz und Vertrauen zu schaffen, um den Koalitionsvertrag umzusetzen, aber auch mit einer präventiven Zielrichtung hat die Polizei in Niedersachsen sämtliche 114 Standorte der polizeilichen Videoanlagen im öffentlichen Raum im Internet veröffentlicht. Die gesetzliche Grundlage für die Maßnahmen ist § 32 Abs. 3 Satz 1 und 2 des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung (Nds. SOG). 76 der Kamerastandorte, also gut zwei Drittel, befinden sich im Zuständigkeitsbereich der Polizeidirektion Hannover. Minister Boris Pistorius erläuterte: „Die Polizei Hannover veröffentlicht die Standorte ihrer Videoüberwachungsanlagen bereits seit geraumer Zeit im Internet. Deshalb ist es richtig, dass dieser Service jetzt auch über die Landeshauptstadt hinaus in ganz Niedersachsen angeboten wird. Durch die ständige Aktualität des Videoanlagenkatasters im Internet stellen wir eine dauerhafte Stärkung der Bürgerrechte sicher, die das Vertrauen der Bürgerinnen und Bürger in die Polizei und deren Transparenz weiter stärkt." Das Videoanlagenkataster wird fortlaufend aktualisiert (Innenministerium Niederachsen, PE 16.10.2014, Pistorius: „Videoanlagenkataster für mehr Transparenz und Stärkung der Bürgerrechte", Kataster: http://www.polizei.niedersachsen.de/aktuelles/videoueberwachung/videoueberwachung-der-polizei-niedersachsen-110205.html).

Nordrhein-Westfalen

LDI informiert über Zulässigkeit privater Videoüberwachung

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) hat eine über 100seitige Broschüre mit dem Titel „Sehen und gesehen werden" veröffentlicht, die unter www.ldi.nrw.de heruntergeladen oder in Papierform kostenfrei bestellt werden kann. Diese gibt Auskunft, was rechtlich zulässig und zu beachten ist. Sie erläutert die gesetzlichen Grundlagen anhand von praktischen Beispielen aus den folgenden Bereichen: Wohnumfeld, Gastronomie, Geschäfte, Parkhäuser, Verkehr, Bildungs- und Freizeiteinrichtungen wie Schwimmbäder und Fitnesscenter, Webcams sowie Videoüberwachung am Arbeitsplatz. Ulrich Lepper: „Wenn Personen zu erkennen sind, darf Videotechnik nur unter engen Voraussetzungen eingesetzt werden. Dabei sind berechtigte Interessen für eine Videoüberwachung mit dem Recht abzuwägen, sich in der Öffentlichkeit frei und ungezwungen zu bewegen. Und am Arbeitsplatz ist eine dauernde Beobachtung unzulässig."

Der LDI NRW stellte die Broschüre auch anderen Einrichtungen, die zum Thema Videoüberwachung beraten, zur Verfügung, z. B. Polizeibehörden, Ordnungsämtern, Schiedspersonen und Verbänden. Ulrich Lepper: „Ich hoffe, dass mit diesem Informationsangebot das Wissen über die Voraussetzungen und Grenzen der Videoüberwachung in NRW verbessert wird. Mich erreichen immer mehr Beschwerden. In schwerwiegenden Fällen verhänge ich Bußgelder – zuletzt über 50.000 Euro gegen ein bundesweit tätiges Unternehmen, das Beschäftigte und Kundschaft überwacht hat. Allerdings kann ich leider nicht allen Beschwerden und Beratungsanfragen im Detail nachgehen. Mit dem neuen Informationsangebot können nun alle, die Videotechnik einsetzen möchten, zunächst selbst beurteilen, ob eine Videoüberwachung zulässig ist, und ihrer Verantwortung für die Einhaltung des Gesetzes gerecht werden" (PE LDI NRW v. 22.9.2014, Videoüberwachung durch Private in NRW – Landesdatenschutzbeauftragter informiert über Voraussetzungen und Grenzen, Bestellmöglichkeit: https://www.ldi.nrw.de/mainmenu_Service/Bestellformular/index.php).

Thüringen

Klopapier-Affäre in Thüringen führt zu Beamten-Hatz

Im Jahr 2011 wurde im Thüringischen Landeskriminalamt (LKA) ein großer blauer Sack mit Toilettenpapier überwacht. Die Putzfrauen hatten beklagt, dass Papierrollen fehlten. Also montierten Spezialbeamte eine Kamera und eine für 3.000 Euro eigens beschaffte Schleuse, um die Kollegen durch den Staatsschutz überwachen zu lassen. Das Klopapier wurden mit elektronischen Etiketten versehen: Falls der Dieb die Schleuse passiert, würde es piepen. Doch es piepte nie. Der angebliche Täter wurde nie gefasst.

Die Geschichte wurde 2012 publik. Die sogenannte Klopapier-Affäre platzte in die Zeit, in der ständig neue Details dazu bekannt wurden, wie Polizei, Staatsanwaltschaft und Verfassungsschutz bei der Fahndung nach drei bombenbauenden Neonazis versagt hatten. Die LKA-Führung hatte sich bei dem Vorgang über Bedenken ihrer Hausjuristen hinweg gesetzt. Der Landesdatenschutzbeauftragte Lutz Hasse sprach Beanstandungen aus. Die Polizeigewerkschaften empörten sich.

Anfang 2013 versprach LKA-Chef Werner Jakstat Besserung: Bei einem Verdacht gegen Beamte sollten „immer erst alle möglichen Optionen und Alternativen geprüft werden“. Als Jakstat dies äußerte, wusste er von der Hatz, die nach dem angeblichen Verräter der peinlichen Ermittlungen veranstaltet wurde, und an der sich sowohl Verfassungsschutz als auch Staatsanwaltschaft willig beteiligten. Diese Ermittlungen wegen des Verdachts auf Geheimnisverrat begannen am 04.07.2011, als ein Journalist beim LKA wegen der Klopapier-Überwachung erstmals anfragte. Noch am selben Tag wurde eine Liste von etwa 20 Beamten erstellt, die von der misslichen Angelegenheit Kenntnis hatten. Darüber hinaus wurde die Staatsanwaltschaft eingebunden und Strafanzeige „von Amts wegen gegen Unbekannt“ gestellt und intern ermittelt. Da alle möglichen Verdächtigen in Erfurt arbeiteten, wurde das Verfahren an die Polizeidirektion Jena abgegeben. Im Juli erteilte das Innenministerium „die Ermächtigung zur Verfolgung der zur Last gelegten Tat der Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht“.

Am 18.08.2011 kam es zu einem ersten Arbeitstreffen zwischen Staatsanwaltschaft und Polizei in Jena, wo die geplanten Vernehmungen von sieben Beamten besprochen wurden. Schnell fokussierten sich die Ermittlungen aber auf einen bestimmten Polizisten A. Einziges Indiz war, dass er den anfragenden Journalisten kannte. Im Januar 2012 wurde gegen den Verdächtigen A. neben Disziplinar- und Ermittlungsverfahren auch eine sogenannte Sicherheitsüberprüfung durchgeführt – an der üblicherweise das Landesamt für Verfassungsschutz beteiligt ist. Gegen A. strengte man eine sogenannte Ü2, eine „erweiterte Sicherheitsüberprüfung“, an. Dabei werden nicht nur die personenbezogen Daten aller Verfassungsschutzämter und Nachrichtendienste, des Bundeszentralregisters, des Bundeskriminalamtes gezogen. Auch alle Polizeidienststellen der Regionen, in denen der Beamte zuletzt gemeldet war, sind abzufragen. In der Regel wird zusätzlich der Lebenspartner überprüft.

Der Verfassungsschutz beantragte Einblick in die Ermittlungsakten. In dem Schreiben an die Staatsanwaltschaft vom 27.01.2012 begründete der Dienst die Forderung damit, dass möglicherweise aus den Akten auch Erkenntnisse über „zum Beispiel Alkoholabhängigkeiten, psychische Erkrankungen oder Überschuldungen“ gewonnen werden könnten. Schließlich, hieß es, gelte bei einer Sicherheitsüberprüfung nicht der Grundsatz „Im Zweifel für den Angeklagten“, sondern „Im Zweifel für die Sicherheit“. Im Frühjahr 2012 beantragte die Staatsanwaltschaft Erfurt beim Amtsgericht „ohne vorherige Anhörung die Durchsuchung der Person, der Wohnung mit Nebenräumen und der Fahrzeuge“ des Beschuldigten. Das wichtigste Indiz blieb weiterhin die Bekanntschaft von A. mit dem Journalisten.

Das Amtsgericht überzeugte dies nicht und teilte am 04.04.2014 der Staatsanwaltschaft mit, dass jeder mit der Klopapier-Ermittlung irgendwie befasste Beamte als Täter infrage komme. Die Zeugenaussagen ergäben „keine Veranlassung“ für einen Durchsuchungsbeschluss. Der Vorwurf gründe sich „auf nichts anderes als Vermutungen“. Dies sei „erheblich zu wenig“. Die Staatsanwaltschaft legte Beschwerde gegen diese Verweigerung der Durchsuchung ein. Am 01.06.2012 bestätigte die 7. Straf- und Beschwerdekammer des Landgerichts, dass der Kreis der Tatverdächtigen etwa 40 Personen betrage. Es sei deshalb nicht nachvollziehbar, warum nur gegen A. ermittelt worden sei. Die Bekanntschaft des Polizisten mit dem Journalisten reiche als Anhaltspunkt nicht aus. A. habe gegenüber seinen Vorgesetzten den Umgang mit dem Journalisten stets offen gelegt. Der Staatsanwaltschaft blieb nichts anderes übrig, als die Ermittlungen einzustellen.

Inzwischen hat der Datenschutzbeauftragte Hasse eine Prüfung eingeleitet. Ihm gehe es vor allem um die Zusammenarbeit mit dem Verfassungsschutz: „Wir haben Akteneinsicht beantragt.“ Als die Presse über den vorstehenden Vorgang berichtete, empörte sich die Opposition im Landtag von Linke, SPD und Grünen über die „Hexenjagd“, den „Exzess“ und die „Einschüchterung“. Mit der Einschaltung des Verfassungsschutzes, so SPD-Fraktionsvize Dorothea Marx habe die „Fehler-Unkultur“ im LKA und im Innenministerium einen „makabren neuen Höhepunkt“ erreicht. Der grüne Innenpolitiker Dirk Adams meinte: „Es ging nicht um einen Diebstahl, sondern darum, unliebsame und kritische Beamte loszuwerden“. Die Linken-Abgeordnete Katharina König reichte eine parlamentarische Anfrage ein und sprach von der „nicht vorhandenen Demokratiekompetenz des Landesamtes für Verfassungsschutz“. Alle drei genannten Abgeordneten gehörten dem NSU-Untersuchungsausschuss des Landtags an, wo sie bei Zeugenvernehmungen oft auf eingeschüchterte Beamte trafen.

Das Innenministerium bemühte sich erst spät um mediale Schadensbegrenzung. Zunächst hatte man noch nicht mitteilen können, warum der Verfassungsschutz an den Ermittlungen gegen den Polizisten beteiligt war. Der für den Geheimschutz zuständige Mitarbeiter des Landeskriminalamtes (LKA) befinde sich im Urlaub, hieß es. Als der Vorgang in der Zeitung stand, wusste

man plötzlich, dass die „Sicherheitsüberprüfung“ im Rahmen der Ermittlungen „erforderlich“ gewesen sei. Für eine andere Entscheidung der Behörden habe es „keinen Spielraum“ gegeben. Später reichte der Ministeriumssprecher am Telefon nach, dass damals für den betroffenen LKA-Beamten aus dienstlichen Gründen sowieso eine erneute Sicherheitsüberprüfung angestanden hätte. Diese sei aufgrund des Verdachts nur noch „vorgezogen“ worden (Debes, Klopapier-Affäre: LKA ließ Polizisten von Geheimdienst überprüfen, www.thueringer-allgemeine.de 03.09.2014; Dedes, Klopapier-Affäre wird zum Thema im Thüringer Landtag, www.thueringer-allgemeine.de 04.09.2014).

Datenschutznachrichten aus dem Ausland

UNO

Menschenrechtsausschuss verlangt Rechtsschutz vor NSA-Überwachung

Der UN-Menschenrechtsausschuss nahm in seinem 4. Staatenbericht zur USA und seinen „Abschließenden Beobachtungen“ (Concluding observations) vom März 2014 Stellung zur Massenüberwachung der NSA. Der Ausschuss wacht über die Einhaltung der bürgerlichen und politischen Rechte in den 167 Ländern, die dem so genannten UN-Zivilpakt beigetreten sind.

Der Ausschuss fordert die USA grundsätzlich dazu auf, die Verpflichtungen des Paktes – entsprechend der Spruchpraxis des Ausschusses und seinem General Comment No. 31 aus dem Jahre 2004 – auch dann einzuhalten, wenn staatliche Stellen der USA außerhalb der USA agieren oder von den USA aus nicht in den USA aufhältige Ausländer „ins Visier“ nehmen. Er zeigt sich in Bezug auf die massenhafte Überwachung der NSA im Rahmen des Überwachungsprogramms PRISM „besorgt“ in Bezug auf den nachteiligen Auswirkungen, die dies auf das Recht der Privatsphäre hat. Er bemängelt insbesondere, dass es in den USA an einem effektiven Instrumentarium für Betroffene sogenannten „non-US persons“ (also Nicht-US-Bürger und Ausländer, die kein Daueraufenthaltsrecht in den USA haben) fehle, um sich gegen die Überwachungsmaßnahmen der NSA rechtlich zur Wehr zu setzen. Der Ausschuss begrüßt zwar, dass Präsident Obama mit seiner Presidential Policy Directive vom 17.01.2014 einen gewissen Schutz auf für non-US persons in Aussicht stellt, macht aber gleichwohl deutlich, dass diese unklaren Aussagen („to the maximum extent feasible consistent with national security“) keinen hinreichenden Schutz bieten.

In seinen Empfehlungen verlangt der Ausschuss, dass die rechtlichen Voraussetzungen für die Überwachung von In- wie Ausländern den gleichen rechtsstaatlichen Grundsätzen, insbesondere dem Grundsatz der Verhältnismäßigkeit genügen müssen. Hierzu verlangt der Ausschuss, dass es eine klare und transparente Rechtsgrundlage gibt, die auf einen spezifischen Zweck ausgerichtet ist und hinreichend präzise die Voraussetzungen und Umstände umschreibt, in denen eine Überwachung zulässig ist. Des Weiteren fordert der Ausschuss Regeln für die Dauer der Überwachung, Verfahren für die Nutzung und Speicherung der Daten sowie Sicherungsmechanismen gegen Missbrauch.

Der Ausschuss empfiehlt eine Reform, die eine wirklich unabhängige und effektive Kontrolle der Überwachung zum Ziel hat. Dies zielt gegen das US-System des geheimen Foreign Intelligence Surveillance Court (FISC), dem der Ausschuss diese Rolle offenbar nicht mal im Ansatz zutraut.

Auch wenn nicht zu erwarten ist, dass sich die USA an alle Empfehlungen des Ausschusses halten werden, so zeigt die Presidential Policy Directive, bei aller Unzulänglichkeit, dass sich die USA zumindest unter einem gewissen Rechtfertigungszwang sehen. Das haben auch die in der Folge zusätzlich gemachten Ankündigungen einer weiteren Verbesserung bezüglich des Rechtsschutzes von Nicht-US-Bürgern gezeigt. Die erfreulich klaren Aussagen des Ausschusses sind jedenfalls ein weiteres, sehr deutliches Signal, dass sich die USA mit ihrer Überwachungspraxis außerhalb des völker- und menschenrechtlich Gebotenen bewegt. Die Stellungnahme des Ausschusses sollte auch der Bundesregierung ein Ansporn sein, endlich ernsthaft gegenüber den USA auf eine Beendigung der massenweisen Verletzung von Grund- und Menschenrechten hinzuwirken (von Notz, UN bestätigt noch einmal: Massenhafte Überwachung widerspricht Menschenrecht gruen-digital.de 30.07.2014; siehe auch zum Bericht der UN-Hochkommissarin vom 16.07.2014 DANA 3/2014, 119 f.).

OECD

„Ende des Bankgeheimnisses“ durch Steuerabkommen

Auf der „Berlin Tax Conference 2014“ haben Vertreter von 51 Staaten ein Abkommen unterschrieben, das Steuerbetrug durch Auslandskonten besser bekämpfen soll. Es regelt ein Verfahren für einen automatischen Daten-Informationsaustausch von Finanzinstituten an Steuerverwaltungen anderer Länder. Ziel ist es, ein Verfahren zu etablieren, das als globaler Standard Verbreitung findet. Das Abkommen auf Initiative der Organisation für Entwicklung und Zusammenarbeit (OECD) basiert auf Ersuchen der G8- und der G20-Staaten. Bisher läuft der Informationsaustausch über Kapitaleinkünfte zum Zweck der korrekten Versteuerung zäh: Hat ein Deutscher beispielsweise in Norwegen ein Konto mit Zinseinkünften, muss er

das zwar in der Steuererklärung angeben. Doch wenn er es nicht tut, ist die Wahrscheinlichkeit, dass diese Einnahmen auffliegen, bisher sehr gering. Die deutschen Steuerbehörden müssten gezielt in Norwegen nachfragen.

Mit den neuen Regelungen sollen die Steuerbehörden in Deutschland automatisch von den Finanzinstituten und Versicherungsgesellschaften in den Unterzeichnerstaaten alle Angaben über Kapitalerträge und den Kontostand ihrer Einwohner bekommen, was die OECD veranlasst zu verkünden: „Die Ära des Bankgeheimnisses ist vorbei." Angaben sind zu machen über Zinsen, Dividenden, Guthaben auf Konten oder Erlöse aus dem Verkauf von Finanzvermögen. Die Meldung erfolgt gegenüber einer Behörde im eigenen Land, wenn der Begünstigte im Ausland lebt. Vom Informationsaustausch betroffen sind nicht nur Einzelpersonen, sondern auch juristische Personen, also Einzelfirmen Stiftungen und Trusts, die oft zur Verschleierung von Identitäten genutzt wurden und von denen künftig die wahren Eigentümer ermittelt und angegeben werden müssen.

Zu den Unterzeichnern gehören große Industriestaaten wie Deutschland, Frankreich und Großbritannien sowie wichtige Finanzzentren wie die Schweiz, Liechtenstein und Singapur sowie diverse Karibik- und Kanalinseln, die traditionell als Heimat von so genannten Briefkastenfirmen dienten, z. B. der Inselstaat Cayman Islands. Alle EU-Staaten sind dabei. Diese hatten untereinander bereits ein entsprechendes System vereinbart. 100 weitere Länder haben das Papier zwar nicht unterzeichnet, befürworten aber die darin aufgeführten Maßnahmen. In vielen Staaten hatten Fälle prominenter Steuerhinterzieher – wie in Deutschland Uli Hoeneß – Empörung hervorgerufen.

Der Austausch zwischen den Unterzeichnerstaaten – die USA gehören nicht dazu – soll auf dem Prinzip der Gegenseitigkeit beruhen. Letztlich verabreden die Staaten über bilaterale Verträge, sich gegenseitig die steuerlich relevanten Daten ihrer Einwohner zukommen zu lassen. Offen ist noch, ob Unterzeichnerstaaten letztlich aussuchen können, mit welchem Unterzeichnerland sie diese Vereinbarung treffen und mit welchem nicht. Sanktionen bei Nichtumsetzung des Abkommen sind nicht vorgesehen. Bei dem US-amerikanischen Anti-Steuerflucht-Abkommen war eine wesentliche Erfolgsbedingung, dass Banken, die aus dem Ausland amerikanische Kunden nicht melden, eine Strafe in Höhe von 30% ihrer US-Einnahmen droht, so dass die Banken ein Eigeninteresse an der Meldung der Daten haben.

Gemäß dem nun verabschiedeten OECD-Abkommen sollen ab 2017 jährlich die Daten des Vorjahres gemeldet werden. Beträge unter 250.000 US-Dollar fallen nicht unter die Informationspflicht. Auch Anteile an Trusts oder Stiftungen von 25% oder weniger müssen nicht gemeldet werden. Die Daten dürfen allein für die Steuererhebung genutzt werden. Zur Verfolgung von Geldwäsche oder Korruption dürfen die Daten nur verwendet werden, wenn die Behörden des Landes, in dem das Geld auf der Bank liegt, dies erlauben. Die neue Regelung gilt für neue Konten, die ab Januar 2016 eröffnet werden. Von September 2017 an können Länder die erhobenen Daten dann untereinander austauschen. In dem Abkommen wird auch ein technischer Rahmen für den Finanzdatenaustausch vorgegeben.

Daneben regelt das Abkommen auch die Rechte und Pflichten bei speziellen und spontanen Anfragen von Behörden aus einem anderen Staat. Den Angaben des Bundesfinanzministeriums nach wird nun explizit ausgeschlossen, dass Staaten die Beantwortung solcher Anfragen weiterhin mit der Begründung verweigern können, die entsprechenden Informationen befänden sich beispielsweise im Besitz eines Kreditinstituts. Der deutsche Bundesfinanzminister Schäuble meinte: „Das Entdeckungsrisiko für Steuersünder wird sehr hoch sein." Gleichwohl werde sich das Problem jedoch nicht komplett abschaffen lassen. Es werde immer wieder Menschen geben, so Schäuble, „die neue Ideen entwickeln, bei der Steuer zu betrügen." In Deutschland wird voraussichtlich das Bundeszentralamt für Steuern die Daten aus dem Ausland empfangen und an die lokalen Finanzämter weitergeben. Ökonomen schätzen, dass Deutsche 360 Mrd. Euro undeklariert im Ausland verbergen.

Trotz einiger Schlupflöcher (fehlende Sanktionen gegen Banken bei lascher Identifizierung und Meldung der tatsächlichen Kontoinhaber, Möglichkeit der Verschleierung über Briefkastenfirmen und Stiftungen, Anlage von Schwarzgeld in Kunst oder Gold) sehen Experten in dem Abkommen einen Meilenstein. Entscheidend ist allerdings, ob es tatsächlich in all den Ländern, die nun unterschrieben haben, auch umgesetzt wird. Auch Aktivisten für mehr Steuergerechtigkeit begrüßten das Abkommen. Manche kritisieren jedoch, dass nicht alle Staaten vom automatischen Informationsaustausch profitieren. Insbesondere arme Entwicklungsländer in Afrika und Asien sind technisch nicht in der Lage, selbst Kundendaten ins Ausland zu liefern.

Wie sensibel die Länder beim Thema Bankengeheimnis sind, zeigt die EU-Zinsrichtlinie: Über zehn Jahre lang wurde in der EU um ein Abkommen gerungen, um zwischen den Mitgliedstaaten einen automatischen Informationsaustausch zumindest über Zinseinkünfte aufzubauen. 2003 trat das Gesetz in Kraft. Die Banken der britischen Inseln Isle of Man, Jersey und Guernsey legen erst seit 2011 die Zinseinkünfte ihrer Auslandkunden den Steuerbehörden offen, Luxemburg und Österreich aber sind immer noch außen vor (Anthony/Meyer-Rüth, „Ära des Bankgeheimnisses ist vorbei", www.tagesschau.de 29.10.2014; Böhme, OECD-Abkommen gegen Steuerflucht, www.dw.de 29.10.2014; Brinkmann, Bankgeheimnis wird bald Geschichte SZ 30.10.2014, 1).

Dänemark

Peilsender-Pilot-Projekt für Obdachlose

Odense, die drittgrößte Stadt in Dänemark, stattet Obdachlose, darunter auch psychisch, Demenz- und Drogen-Kranke, mit Peilsender aus, um diese auf der Straße lebenden Menschen zu überwachen. Die Daten gehen direkt an eine städtische Behörde, die Bewegungsabläufe und Aufenthaltsorte der Obdachlosen auswertet. Als Anreiz dafür, dass sie einen Peilsender in der Tasche tragen, erhalten sie drei warme

Mahlzeiten pro Tag. Sozialarbeiter Tom Roenning, der das Projekt initiiert hat, erläutert: „So weit ich weiß, wurde das weltweit noch nie zuvor getestet. Das Ziel ist, möglichst viel über das Leben der Obdachlosen zu erfahren – wir wollen wissen, wohin sie gehen, wann sie dort hingehen, wie lange sie bleiben.“

Die Verantwortlichen in Odense bemühen sich, die guten Absichten hinter dem orwellsch anmutenden Projekt herauszustellen. Steen Moller, konservativer Vizebürgermeister, weist darauf hin, dass alles auf freiwilliger Basis stattfindet. Die Stadt sammle die Daten nicht, um Obdachlose aus der Öffentlichkeit zu verdrängen oder sie zu drangsalieren. Vielmehr gehe es darum, das Leben auf der Straße zu verbessern: „Solange das freiwillig geschieht, ist es eine Situation, die für alle von Vorteil ist.“ Roenning ergänzt: „Indem wir die bevorzugten Plätze und den Tagesrhythmus wohnungsloser Menschen kennen, können wir unsere sozialen Hilfsangebote verbessern.“ Wärmstuben, medizinische Hilfen und resozialisierende Aktionen könnten zum richtigen Zeitpunkt an den städtischen Routen und Treffpunkten der Obdachlosen optimal platziert werden. Bislang habe es Sozialarbeitende gegeben, die gelegentlich mit Listen durch die Stadt liefen, um Aufenthaltsorte der Obdachlosen zu notieren. Das Sozialbudget könne effektiver eingesetzt werden. Auch für Angehörige der Obdachlosen, die sich Sorgen machen, könnten GPS-Sender eine gewisse Erleichterung bringen.

Was in anderen Ländern Alarmglocken schrillen lässt, trifft in Dänemark kaum auf Kritik. In Skandinavien trauen die Menschen traditionell ihrem Staat. Wenn der Wohlfahrtsstaat Gutes für sie tut, müssen sich die Menschen auch überwachen lassen, so eine weit verbreitete Meinung. Den Initiatoren war von Anfang an bewusst, dass das Projekt auf ethische Vorbehalte stoßen könnte. So heißt es, dass die GPS-Ortung anonym sei: Welcher Obdachlose welchen Peilsender trägt, werde nicht erfasst. Eine individuelle Verfolgung der Teilnehmenden, so Roenning, sei demnach gar nicht möglich. Zudem sei die Datenerfassung zeitlich begrenzt. Eine Woche lang werden die Standorte der Obdachlosen aufgezeichnet, alle sechs Monate soll die Messung wiederholt werden. 20 Personen haben am ersten Durchlauf des Projekts teilgenommen, der im September 2014 beendet wurde. Negative Reaktionen blieben bisher aus. Dänische Medien berichten positiv über das Projekt. Roenning: „Wir haben uns bemüht, alle Beteiligten von Anfang an über die Maßnahme zu informieren und sie einzubeziehen.“ Besonders die Obdachlosen hätten mit Begeisterung auf das Projekt reagiert. Die Überwachung werteten sie als Interesse für ihre Bedürfnisse, nicht als Eingriff in die Privatsphäre.

Ursprünglich wurden die GPS-Sender zum Schutz von Demenzkranken, die sich nicht mehr allein orientieren können, entwickelt. Dass diese Technik nun in der Obdachlosenhilfe angekommen ist, findet Roenning mit Blick auf die Stadtentwicklung logisch: „Heute sind viele Plätze in der Stadt privatisiert, Obdachlose müssen ständig ihren Schlafplatz wechseln. Vor diesem Hintergrund ist es für Sozialarbeiter schwierig, Wohnungslose zu finden und regelmäßige Hilfe zu leisten.“ Schätzungen zufolge leben heute zwischen 10.000 und 15.000 Menschen in Dänemark auf der Straße, die meisten in Kopenhagen. In Odense sind ca. 1% der 187.000 BewohnerInnen ohne eigenen Wohnsitz, die meisten von ihnen sind bereits in städtischen Unterkünften untergebracht. Laut einer Studie des Danish National Centre for Social Research haben sich die Obdachlosenzahlen in Odense von 2009 bis 2013 halbiert – Experten loben die städtischen Behörden für die schnelle Vermittlung in Privatwohnungen und die gute Sozialberatung für Obdachlose.

Das Projekt löste eine öffentliche Debatte über den Umgang mit Obdachlosen in Dänemark aus. Die Behörden in Odense setzen auf Verständigung und Integration – und stellen sich damit gegen den Trend zur Verdrängung von Obdachlosen, der in vielen europäischen Städten zu beobachten ist. In Madrid etwa sollen 4.000 Busstationen so umgebaut werden, dass Obdachlose nicht mehr auf den Sitzbänken schlafen können. In der Stadt, die von der Finanzkrise hart getroffen wurde und in der viele soziale Einrichtungen schließen mussten, löste die Maßnahme Empörung aus. Roenning beobachtet diese Entwicklung mit Sorge: „Ausschluss ist das falsche Signal. So werden obdachlose Menschen niemals wieder in die Gesellschaft integriert.“ Wer helfen wolle, müsse das Leben der Obdachlosen zunächst verstehen – und dann zentrale Hilfsangebote schaffen, anstatt soziale Probleme aus dem öffentlichen Bewusstsein zu verdrängen. Die GPS-Überwachung in Odense soll nun dabei helfen. Im Dezember 2014 werden dann erneut Peilsender an Obdachlose in der Stadt verteilt (Anwar, Kieler Nachrichten 27.09.2014, 13; Lasarzik, Pilot-Projekt in Dänemark: Peilsender für Obdachlose, www.spiegel.de 23.09.2014).

Türkei

Neue Regierung verschärft Internetkontrolle weiter

Der türkische Präsident Recep Tayyip Erdoğan hatte in den letzten Monaten seiner Amtszeit als Premierminister keinen Zweifel daran gelassen, was er von den sozialen Netzwerken hält: Der Kurznachrichtendienst Twitter sei eine „große Gefahr“, müsse an „der Wurzel“ ausgerissen werden und diene als „Mittel für systematischen Rufmord“. Im Februar 2014 hatte die damalige türkische Regierung schon ein Gesetz zur schärferen Internetkontrolle durchgesetzt. Die neue türkische Regierung unter Premierminister Davutoğlu baut diese Internet-Kontrolle aus und nutzt hierfür die Parlamentsmehrheit der Regierungspartei AKP. Am 09.09.2014 verabschiedete das Parlament ein Gesetz, das über die bestehende restriktive Regelung insbesondere in zwei Punkten hinausgeht. Künftig darf die staatliche Telekommunikationsbehörde TIB Websites ohne Gerichtsbeschluss sperren, zum Schutz der nationalen Sicherheit, um die öffentliche Ordnung wiederherzustellen oder um Verbrechen zu verhindern – Formulierungen mit viel Spielraum für die Auslegung. Erst nach der Sperrung muss sich die Behörde innerhalb von 24 Stunden an ein Gericht wenden, das die Blockade – wiederum innerhalb einer 48-Stunden-Frist – genehmigen muss. Bisher war das Sperren von Internetseiten ohne vorherigen Gerichtsbeschluss nur zulässig, wenn

eine eindeutige Verletzung von Persönlichkeitsrechten vorlag.

Das neue Gesetz sieht zudem vor, dass TIB Nutzerdaten bis zu zwei Jahre auf Vorrat speichern darf. Bisher galt eine zweijährige Speicherpflicht für Dienstanbieter; die staatliche TIB durfte diese Daten abfragen, wenn im Rahmen von Ermittlungen ein richterlicher Beschluss vorlag. Mit der neuen Regelung darf die Behörde Nutzerdaten anfordern oder erheben, speichern und entsprechend schnell darauf zugreifen; sie darf diese Daten zudem an die Sicherheitsdienste weitergeben – benötigt dafür allerdings einen Gerichtsbeschluss.

Erdal Aksünger, Abgeordneter der größten Oppositionspartei CHP, meinte, die Türkei werde ein Ort, „in dem Gesetzesänderungen über Nacht vorgenommen werden, um das Land nach Gestapo-Manier zu regieren“. Die neue Macht der TIB-Behörde schaffe die Gewaltenteilung ab. Der Internet-Experte Kerem Altıparmak warnte, mit dem Gesetz könne der Vorsitzende der Internetbehörde willkürlich gegen Websites vorgehen, die ihm nicht gefielen. Und die Menschenrechtsorganisation Human Rights Watch kritisierte das Gesetz als „Eingriff in die Privatsphäre aller Internetnutzer“. Die Zustimmung von Erdoğan zu dem vom Parlament verabschiedeten Gesetz gilt als sicher, zumal er es war, der im Frühjahr eine Sperre von Youtube und Twitter angeordnet hatte, nachdem Telefonmitschnitte und Korruptionsvorwürfe gegen ihn im Netz die Runde machten, etwa eine Aufnahme, in der er angeblich seinen Sohn anweist, Schmiergelder zu verstecken. Das Verfassungsgericht hob die Sperre der Seiten später wieder auf (Seeling, Schlag gegen Websites, SZ 11.09.2014, 7; Regierung verschärft Internet-Kontrolle, www.sueddeutsche.de 12.09.2014).

Israel

Reservisten von Spionage-Elite verweigern sich

In einem Brief an den israelischen Ministerpräsidenten Benjamin Netanjahu und die Armeeführung, Verteidigungsminister Mosche Jaalon, schrieben 43 Soldaten und Reservisten der Elite-Aufklärungseinheit „Einheit 8200“, sie wollten nicht länger die Rechte von Millionen Menschen verletzen und sich nicht weiter an Einsätzen beteiligen, die sich gegen die Palästinenser richten. In dem Brief werfen die Soldaten der Regierung vor, die Informationen der Einheit zu nutzen, um unschuldigen Zivilisten zu schaden. Die Daten ermöglichten politische Verfolgung und spalteten die palästinensische Gesellschaft durch das Anwerben von Informanten. Die Reservisten innerhalb der Einheit würden den Dienst deswegen verweigern: „Wir können nicht mit gutem Gewissen weiterhin in diesem System dienen.“ Die palästinensische Bevölkerung sei der Überwachung und Spionage von israelischer Seite vollkommen schutzlos ausgesetzt. „Während es strenge Grenzen bei der Überwachung der israelischen Bevölkerung gibt, genießen die Palästinenser diesen Schutz nicht.“ Es werde kein Unterschied zwischen Menschen mit und ohne gewalttätigen Hintergrund gemacht. Die Arbeit des israelischen Geheimdienstes mache es den Menschen in den besetzten Gebieten unmöglich, ein normales Leben zu führen. Die Autoren betonen, sie seien keinesfalls generell gegen die Geheimdienstarbeit oder die Armee, sondern nur gegen die Auswüchse der Besatzung.

Die Unterzeichner arbeiten in der „Einheit 8200“ der Streitkräfte, die für die elektronische Aufklärung zuständig ist. Sie ähnelt in ihrer Arbeit dem US-amerikanischen Geheimdienst National Security Agency (NSA). Aufgabe der dort arbeitenden Soldaten ist es Telefonate abzuhören, E-Mails und den SMS-Verkehr abzufangen. In dem Brief heißt es, dass ein großer Teil ihrer Arbeit nichts mit der Sicherheit Israels zu tun gehabt habe. Vielmehr sei es darum gegangen, alle Aspekte des palästinensischen Lebens zu kontrollieren, um so die Besetzung aufrecht zu erhalten. Es würden Informationen über sexuelle Vorlieben oder Krankheiten gesammelt, um Palästinenser zu erpressen und zu Kollaborateuren zu machen. Dies diene zwar manchmal der Gefahrenabwehr, doch dabei würden die „Rechte von Millionen Menschen“ verletzt. „Wir weigern uns, ein Werkzeug zu sein, das die militärische Kontrolle der besetzten Gebiete vertieft.“ Alle Soldaten und überhaupt alle israelischen Bürgerinnen und Bürger werden aufgefordert, „ihre Stimme gegen diese Verstöße zu erheben und ihnen ein Ende zu setzen“. Zu den Beweggründen für den Schritt an die Öffentlichkeit erklärte einer der Autoren, er habe den Film „Das Leben der Anderen“ gesehen, in dem es um die Methoden der Stasi in der DDR geht: „Wir tun genau dasselbe, nur effizienter.“

Die Armee drohte den Soldaten daraufhin mit harten disziplinarischen Maßnahmen. Geheimdienstminister Juval Steinitz will sie vor Gericht stellen. Regierungschef Netanjahu reagierte auf den Brief, indem er von „haltlosen Verleumdungen“ sprach und die Truppe pauschal als „moralischste Armee der Welt“ bezeichnete. Präsident Reuven Rivlin stellte sich vor die „Einheit 8200“ und forderte sie auf, ihre „wichtige Mission“ unbeirrt fortzuführen. Verteidigungsminister Jaalon bescheinigte der Eliteeinheit eine „heilige Arbeit, die schon viele Leben gerettet“ habe. Er beauftragte den Generalstabschef, die Brief-Autoren als Straftäter zu behandeln. Parlamentspräsident Juli Edelstein warf den Briefschreibern vor, „all jenen einen hervorragenden Dienst zu erweisen, die Israel hassen“. Oppositionsführer Issac Herzog von der Arbeitspartei, selbst ehemals Major bei der „Einheit 8200“, bekundete über Facebook seine Treue zur alten Truppe und verurteilte aufs Schärfste diesen „Aufruf zum Ungehorsam“. Wenn es Missstände gebe, müssten diese auf anderem Weg als durch Befehlsverweigerung angesprochen werden. Lediglich Zehava Galon von der linken Meretz-Partei, brach eine Lanze für die Reservisten: „Eine Regierung, die ihre besten Söhne in den Krieg schickt, sollte auch darauf hören, was sie zu sagen haben.“ Wenn die Verweigerer vor Gericht gestellt werden, droht ihnen eine Gefängnisstrafe bis zu drei Jahren (Münch, Sturm der Entrüstung, SZ 16.09.2014, 8; Israelische Elite-Einheit verweigert Spionage gegen Palästinenser, www.zeit.de 12.09.2014, Elite-Soldaten verweigern Einsätze gegen Palästinenser, www.sueddeutsche.de 12.09.2014).

USA

Yahoo drohte Millionenstrafe bei Datenverweigerung

Yahoo veröffentlichte am 11.09.2014 Dokumente aus seinem Widerspruchsverfahren vor dem Geheimgericht Foreign Intelligence Surveillance Court (FISC). Danach sollte das Unternehmen verpflichtet werden, täglich 250.000 US-Dollar zu zahlen, falls es die massenhafte Weitergabe von Userdaten an US-Geheimdienste verweigerte. Die US-Regierung hat Yahoo 2008 mit dieser millionenschweren Geldbuße gedroht, falls der Internetkonzern die massenhafte Weitergabe von Nutzerdaten an die Geheimdienstbehörden verweigern sollte. Das Unternehmen wollte nicht der Aufforderung zur Datenübermittlung nachkommen, die es als verfassungswidrig ansah.

Yahoo hatte gemäß den Angaben von Yahoo-Chefjustiziar Ron Bell die entsprechenden US-Überwachungsgesetze beim FISC angefochten: „Unsere Anfechtung und eine spätere Berufung in dem Fall waren nicht erfolgreich." Die Niederlage führte schließlich dazu, dass Yahoo und sieben andere Firmen beim Prism-Programm des Geheimdienstes NSA mitmachen mussten, das zur Sammlung von Millionen Nutzerdaten diente. Dass die rund 1500 bislang geheim gehaltene Seiten des damaligen Verfahrens freigegeben wurden, ist für Yahoo ein Erfolg, so Bell: „Wir halten es für einen wichtigen Sieg für die Transparenz. Die User kommen zuerst bei Yahoo." Das Unternehmen will die Schriftstücke nach und nach publizieren, da das Gericht selbst keinen öffentlichen Zugang zu freigegebenen Schriftstücken biete und Yahoo die Dokumente für die Web-Pulbikation tauglich machen müsse. Außerdem erklärte Bell, dass trotz der Freigabe der Dokumente Teile davon weiterhin unter Verschluss blieben – nicht einmal Yahoo bzw. die Juristen von Yahoo würden diese Teile kennen. Yahoo will weiterhin Anordnungen und Gesetze anfechten, die man als unrechtmäßig, unklar oder zu weit gefasst ansehe (NSA-Überwachungsskandal: Millionenstrafe für Yahoo bei Nicht-Herausgabe von Nutzerdaten, www.heise.de 12.09.2014; US-Regierung drohte Yahoo, SZ 13./14.09.2014, 10).

USA

Internetvollprofil für 100 Dollar im Monat

In den USA können KundInnen sich gegen Bezahlung von einer Marktforschungsfirma überwachen lassen. Die weiß dann immer, wohin man surft und wo man sich befindet. Luth Research, eine Firma aus San Diego, will Marketingunternehmen und Werbetreibenden Zugriff auf das digitale Leben Zehntausender Menschen geben, die sich vorher bereiterklärt haben, mitzumachen. Sie erhalten 100 Dollar im Monat, sollen dafür den Großteil ihrer Aktivitäten auf Smartphone, Tablet oder PC offenlegen. Luth nennt das Angebot „ZQ Intelligence". Es sammelt und analysiert Daten von den Telefonen und Computern vorausgewählter Teilnehmer über ein geschütztes virtuelles privates Netzwerk (VPN). Die Daten werden durch die Server der Firma geschleust, gesammelt und auf Trends analysiert. Luth schaut sich laut eigenen Angaben nicht die Inhalte von Nachrichten an, weiß aber beispielsweise, wo sich die Smartphone-Nutzenden gerade aufhalten, welche Websites sie anklicken, nach was sie bei Google suchen und wie oft sie Twitter checken. Die Teilnehmenden müssen außerdem regelmäßig Fragen über ihr Onlineverhalten beantworten.

Luth führte z. B. im Jahr 2013 ein Projekt für den Autohersteller Ford durch, der genauer wissen wollte, wie die Kaufentscheidung für einen Neuwagen bei den KundInnen fällt. Luth suchte daraufhin nach KundInnen, die sich gerade für ein Fahrzeug interessieren – und verfolgte ihren digitalen Weg von den ersten Recherchen im Web bis zum tatsächlichen Kauf. Dabei war z. B. nachvollziehbar, wann ein Kunde zu einem Händler fuhr und dort dann die Websites konkurrierender Autohersteller auf seinem Mobiltelefon besuchte. Auch das Auffinden von Finanzierungsoptionen wurde getrackt (Vollzugriff auf Onlinedaten für 100 Dollar im Monat, www.heise.de 16.10.2014).

Venezuela

Fingerabdrücke gegen Schmuggel

In allen Supermärkten Venezuelas sollen gemäß den Vorstellungen von Staatspräsident Nicolas Maduro künftig Fingerabdruck-Scanner an den Kassen stehen, mit denen festgestellt werden wird, ob einzelne BürgerInnen ungewöhnlich häufig und viel einkaufen. Dahinter steht der Verdacht, dass die Kaufenden die Produkte außer Landes schmuggeln und dort zu höheren Preisen weiterverkaufen. Die Scanner seien ein „Segen" im Kampf gegen den Schmuggel günstiger Lebensmittel aus Venezuela in die Nachbarstaaten: „Das biometrische System wird perfekt sein." Staatliche Preiskontrollen sorgen in Venezuela dafür, dass Lebensmittel und andere Produkte des täglichen Bedarfs teils nur ein Zehntel so viel kosten wie in den Nachbarstaaten. Maduro führt die grassierende Lebensmittelknappheit darauf zurück, dass in großem Stil günstige Produkte aus Venezuela herausgeschmuggelt werden, insbesondere nach Kolumbien. Seit kurzem schließt Venezuela jede Nacht die 2.200 Kilometer lange Grenze zwischen beiden Ländern. Oppositionspolitiker kritisierten den Scanner-Plan scharf und verglichen ihn mit kommunistischen Rationierungsmaßnahmen, so z. B. der oppositionelle Abgeordnete Alfonso Marquina: „Die Regierung kann Familien nicht einfach sagen, was sie essen sollen." Obwohl Venezuela die größten Ölreserven der Welt hat, steckt die Wirtschaft des Landes seit Langem in der Krise. Die Staatsverschuldung steigt, es gibt ständig Engpässe bei der Versorgung mit Grundnahrungsmitteln und anderen wichtigen Gütern. Die Inflation stand aufs Jahr gerechnet zuletzt bei 60% (Scanner gegen Schmuggel, SZ 23./24.08.2014, 29).

Japan

Polizei konfisziert Spanner-Videoschuhe

In Japan fahndet die Polizei nach mehr als 2.000 Menschen, die Schuhe mit versteckten Minikameras gekauft

haben und damit heimliche Aufnahmen unter Frauenröcken gemacht haben könnten. Die High-Tech-Spannerschuhe konnten via Fernsteuerung bedient werden. Die zuständigen Beamten in der alten Kaiserstadt Kyoto hatten zuvor die Betreiber einer Internetseite, auf der solche Schuhe vertrieben wurden, bereits zu einer Geldstrafe verdonnert. Die Polizei fahndet nun nach allen Käufern, die auf der Kundenliste der Website aufgeführt sind, die sichergestellt wurde. Die Polizei in Kyoto: „Der einzige Weg solche heimlichen Fotos einzudämmen, ist die Geräte auszumerzen.“ Die Beamten klingeln von Tür zu Tür, um die Verantwortlichen zur Aushändigung der Schuhe aufzufordern. Insgesamt sollen etwa 2.500 Paare zwischen den Jahren 2012 und 2014 verkauft worden sein. Ein Paar kostete umgerechnet etwa 215 Euro. Bereits im vergangenen Juli waren in Kyoto sowohl ein Verkäufer als auch ein Kunde vorübergehend festgenommen worden. Beide wurden zu einem Bußgeld von je 500.000 Yen, umgerechnet knapp 3.600 Euro herangezogen (Aktion gegen Spanner, SZ 18.09.2014, 8; High-Tech-Spanner: Polizei fahndet nach Kamera-Schuhen; www.chip.de 17.09.2014).

Rechtsprechung

BGH

IP-Adressenspeicherung für 7 Tage ist okay

Der Bundesgerichtshof (BGH) hat gemäß seinem Urteil vom 03.07.2013 keine Einwände gegen die Praxis der Deutschen Telekom, IP-Adressen als Verbindungsdaten von Internetnutzern eine Woche lang aufzubewahren, um im Einklang mit § 96 Abs. 1 S. 2 i. V. m. § 100 Abs. 1 Telekommunikationsgesetz (TKG) Netzstörungen und Fehler an TK-Anlagen abzuwehren (Az. III ZR 391/13). Der BGH schloss sich damit der Meinung des Oberlandesgerichts Frankfurt (OLG) und eines Sachverständigen an, dass es nach dem derzeitigen Stand der Technik keine andere Möglichkeit zur Garantie der Netzsicherheit gibt und diese Maßnahme verhältnismäßig ist.

Der BGH hatte schon in der gleichen Angelegenheit am 13.01.2011 (Az. III ZR 146/10) ähnlich geurteilt. Kläger war ein DSL-Kunde der Telekom, der von dieser eine dynamische IP-Adresse für den Zugang zum Internet erhält. Er meinte, die Telekom müsse diese Verbindungsdaten aus Datenschutzgründen sofort nach dem Ende der Online-Sitzung löschen. Der BGH bezieht sich in seiner aktuellen Begründung auf die Ausführungen des OLG Frankfurt, wonach der angehörte Experte „nachvollziehbar dargelegt“ habe, dass bei der Telekom monatlich mehr als 500.000 Missbrauchsmeldungen eingingen. Von diesen stünden allein 162.000 im Zusammenhang mit Spam. 164.000 hätten einen potenziell direkten Einfluss auf die Infrastruktur und die Dienste der Telekom. Der BGH wies darauf hin, dass die Telekom schon dann eingeschränkt werde, wenn aufgrund unerwünschter Werbemails einzelne ihrer IP-Nummernbereiche von anderen Internetdiensten gesperrt werden. Die vom Kläger geforderte Pseudonymisierung müsste dann gemäß gesetzlicher Vorgaben aufgehoben werden. Der Sachverständige habe dargelegt, dass der damit verbundene Mehraufwand angesichts der Vielzahl der Fälle, die monatlich abzuwickeln seien, nicht vertretbar sei.

Auch mit EU-Datenschutzvorgaben sei die einwöchige Speicherung vereinbar. Diese sähen eine Ausnahme von Löschungspflichten für Verbindungsdaten bereits zum Verhüten, Ermitteln, Feststellen und Verfolgen von Missbräuchen der Kommunikationssysteme vor, was erst recht für das Erkennen, Eingrenzen oder Beseitigen von hieraus resultierenden Störungen der TK-Anlagen des Netzbetreibers gelten müsse. Das Urteil des Europäischen Gerichtshofs (EuGH) zur Vorratsdatenspeicherung ergäbe kein anderes Ergebnis. Für den EuGH sei das Fehlen eines objektiven Kriteriums zum Aufbewahren von Verbindungsdaten maßgeblich gewesen. Das sei nicht auf die Speicherung bei der Telekom übertragbar, die nicht für Zwecke der Strafverfolgung erfolge, sondern im Interesse des Netzbetreibers (Krempl, BGH bleibt dabei: Siebentägiges Speichern von IP-Adressen ist rechtmäßig, www.heise.de 01.08.2014; NJW 2014, 2500 ff.).

BGH

EuGH-Vorlage: Umgang mit dynamischen IP-Adressen

Mit Urteil vom 28.10.2014 entschied der Bundesgerichtshof (BGH), zwei Fragen zum datenschutzrechtlichen Umgang mit dynamischen IP-Adressen dem Europäischen Gerichtshof vorzulegen (VI ZR 135/13). In dem Verfahren verlangt der Kläger von der beklagten Bundesrepublik Deutschland Unterlassung der Speicherung von dynamischen IP-Adressen. Bei den meisten allgemein zugänglichen Internetportalen des Bundes werden alle Zugriffe in Protokolldateien festgehalten mit dem Ziel, Angriffe abzuwehren und die strafrechtliche Verfolgung von Angreifern zu ermöglichen. Dabei werden unter anderem der Name der abgerufenen Seite, der Zeitpunkt des Abrufs und die IP-Adresse des zugreifenden Rechners über das Ende des jeweiligen Nutzungsvorgangs hinaus gespeichert.

Mit der Klage will der Kläger erreichen, dass die ihm zugewiesenen IP-Adressen nicht über das Ende des jeweiligen Nutzungsvorgangs hinaus gespeichert werden. Das Amtsgericht Tiergar-

ten hatte die Klage am 13.08.2008 abgewiesen (2 C 6/08). Auf die Berufung des Klägers hat das Landgericht Berlin dem Kläger mit Urteil vom 31.01.2013 den Unterlassungsanspruch nur insoweit zuerkannt, als er Speicherungen von IP-Adressen in Verbindung mit dem Zeitpunkt des jeweiligen Nutzungsvorgangs betrifft und der Kläger während eines Nutzungsvorgangs seine Personalien angibt (57 S 87/08). Gegen dieses Urteil haben beide Parteien die vom Berufungsgericht zugelassene Revision eingelegt.

Der BGH beschloss, das Verfahren auszusetzen und dem EuGH zwei Fragen zur Auslegung der EG-Datenschutz-Richtlinie zur Vorabentscheidung vorzulegen:

1. Der Unterlassungsanspruch setzt voraus, dass es sich bei den dynamischen IP-Adressen für die verantwortlichen Stellen der Beklagten, die die Adressen speichern, um „personenbezogene Daten" handelt, die von dem durch die Richtlinie harmonisierten Datenschutzrecht geschützt werden. Das könnte in den Fällen, in denen der Kläger während eines Nutzungsvorgangs seine Personalien nicht angegeben hat, fraglich sein. Denn nach den getroffenen Feststellungen lagen den verantwortlichen Stellen keine Informationen vor, die eine Identifizierung des Klägers anhand der IP-Adressen ermöglicht hätten. Auch durfte der Zugangsanbieter des Klägers den verantwortlichen Stellen keine Auskunft über die Identität des Klägers erteilen. Der Bundesgerichtshof hat dem Europäischen Gerichtshof deshalb die Frage vorgelegt, ob Art. 2 Buchstabe a der EG-Datenschutz-Richtlinie dahin auszulegen ist, dass eine IP-Adresse, die ein Diensteanbieter im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, für diesen schon dann ein personenbezogenes Datum darstellt, wenn lediglich ein Dritter über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt.

2. Geht man von „personenbezogenen Daten" aus, so dürfen die IP-Adressen des Nutzers nicht ohne eine gesetzliche Erlaubnis gespeichert werden (§ 12 Abs. 1 TMG), wenn – wie hier – eine Einwilligung des Nutzers fehlt. Nach dem für die rechtliche Prüfung maßgebenden Vortrag der Beklagten ist die Speicherung der IP-Adressen zur Gewährleistung und Aufrechterhaltung der Sicherheit und Funktionsfähigkeit ihrer Telemedien erforderlich. Ob das für eine Erlaubnis nach § 15 Abs. 1 TMG ausreicht, ist fraglich. Systematische Erwägungen sprechen dafür, dass diese Vorschrift eine Datenerhebung und -verwendung nur erlaubt, um ein konkretes Nutzungsverhältnis zu ermöglichen, und dass die Daten, soweit sie nicht für Abrechnungszwecke benötigt werden, mit dem Ende des jeweiligen Nutzungsvorgangs zu löschen sind. Art. 7 Buchstabe f der EG-Datenschutz-Richtlinie könnte aber eine weitergehende Auslegung gebieten. Der BGH hat dem EuGH deshalb die Frage vorgelegt, ob die EG-Datenschutz-Richtlinie einer Vorschrift des nationalen Rechts mit dem Inhalt des § 15 Abs. 1 TMG entgegen steht, wonach der Diensteanbieter personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben und verwenden darf, soweit dies erforderlich ist, um die konkrete Inanspruchnahme des Telemediums durch den jeweiligen Nutzer zu ermöglichen und abzurechnen, und wonach der Zweck, die generelle Funktionsfähigkeit des Telemediums zu gewährleisten, die Verwendung nicht über das Ende des jeweiligen Nutzungsvorgangs hinaus rechtfertigen kann (Vorlage an den EuGH in Sachen „Speicherung von dynamischen IP-Adressen", BGH PM v. 28.10.2014).

BGH

Arztpraxen müssen Internet-Bewertungen zumeist dulden

Der Bundesgerichtshof (BGH) hat mit Urteil vom 23.09.2014 die Klage eines Münchner Gynäkologen abgewiesen, der seinen Eintrag im Bewertungsportal Jameda.de löschen lassen wollte (VI ZR 358/13). Auch die Vorinstanzen hatten die Klage abgewiesen. Das Landgericht hatte sich in der Abwägung für die Kommunikationsfreiheit des Internetanbieters entschieden. Die beruflichen Daten des Mediziners dürften erhoben, gespeichert und genutzt werden. Der Vorsitzende Richter Gregor Galke erläuterte in der Verhandlung, dass der „Knackpunkt" bei der Abwägung läge, ob das Recht des Arztes auf informationelle Selbstbestimmung stärker wiege als das Recht der Firma auf Kommunikationsfreiheit. Eine Rolle spielte dabei auch das Urteil des BGH von 2009 zum Lehrer-Bewertungsportal „spickmich", in dem die Klage einer Lehrerin gegen ihre Benotung abgewiesen wurde (DANA 2/2009, 75). Zwar werde ein Arzt durch negative Bewertungen „nicht unerheblich belastet", auch weil eine gewisse Gefahr des Missbrauchs solcher Portale bestehe, aber: „Das Recht des Klägers auf informationelle Selbstbestimmung überwiegt das Recht der Beklagten auf Kommunikationsfreiheit nicht." Zu berücksichtigen sei auch „das Interesse der Öffentlichkeit an Informationen über ärztliche Leistungen". Vor dem Hintergrund der freien Arztwahl trage das Portal dazu bei, den PatientInnen die aus seiner Sicht erforderlichen Informationen zur Verfügung zu stellen. Als niedergelassener Arzt wende sich der Kläger an potenzielle PatientInnen und stelle sich damit dem freien Wettbewerb, wo er sich auf Kritik einstellen müsse. Unter diesen Umständen sei der Schutz des Persönlichkeitsrechts nicht sonderlich stark ausgeprägt.

Die vom Portal erhobenen Daten berührten einen Bereich, in dem „sich der Einzelne auf die Beobachtung seines Verhaltens durch eine breitere Öffentlichkeit sowie auf Kritik einstellen" müsse. Dabei sei der Beklagte nicht schutzlos, weil er die Löschung unwahrer Tatsachenbehauptungen sowie beleidigender oder sonst unzulässiger Bewertungen verlangen könne. Im Juli 2014 hatte der BGH über die Klage eines anderen Arztes entschieden, der auf dem Portal Sanego mehrfach anonym mit übler Nachrede überzogen worden war. Das Portal löschte gemäß seiner Verpflichtung diese Einträge, die unwahre Behauptungen oder stigmatisierende Bewertungen enthielten. In dem Fall hatte der BGH aber das Auskunftsverlangen gegenüber dem Portal über Name und Anschrift des Anonymus zurückgewiesen. Ein Anspruch auf Herausgabe der Nutzerdaten möge zwar „wünschenswert" sein, doch das müsse der Gesetzgeber entscheiden. Inzwischen hat die CDU-Bundestagsfraktion den Hinweis aufgegriffen und will den Schutz vor Verleumdungen verbessern,

indem im Wiederholungsfall die Identität anonymer Kritiker aufgehoben wird. In der aktuellen BGH-Verhandlung berichtete der Anwalt des klagenden Arztes Joachim Kummer, auf jameda.de würden Ärzte aus dem Umfeld des angeklickten Mediziners angezeigt. Gegen Entgelt werde diese Konkurrenz ausgeblendet. Für den konkret entschiedenen Fall kam diese Information zu spät. Sie hätte schon vor den unteren Instanzen vorgebracht werden müssen (Bundesgerichtshof: Ärzte müssen Online-Bewertungen dulden, www.heise.de 23.09.2014; Janisch, Kein Entrinnen, SZ 24.09.2014, 19).

BVerwG:

Presse hat Anspruch auf Kenntnis der Gerichtspersonen

Das Bundesverwaltungsgericht (BVerwG) hat mit Urteil vom 01.10.2014 entschieden, dass der Presse auf Anfrage regelmäßig die Namen der Personen, die in einem Gerichtsverfahren mitgewirkt haben, mitzuteilen sind (Az. 6 C 35.13). Der Kläger, Redakteur der „Anwaltsnachrichten Ausländer- und Asylrecht", bat den Direktor des Amtsgerichts (AG) Nürtingen, ihm die Abschrift einer strafgerichtlichen Entscheidung zwecks Publikation in dieser Zeitschrift zu übersenden. Er erhielt eine anonymisierte Kopie des Urteils, in der die Namen der am Verfahren mitwirkenden Personen geschwärzt waren (Berufsrichterin und Schöffen, Vertreter der Staatsanwaltschaft, Verteidiger, Urkundsbeamtin der Geschäftsstelle). In der Folge teilte der Direktor des AG dem Kläger den Namen der Berufsrichterin mit, lehnte aber weitere Angaben ab. Die Klage hiergegen wurde vom Verwaltungsgericht VG Stuttgart abgewiesen. Auf die Berufung des Klägers wurde das beklagte Land Baden-Württemberg vom Verwaltungsgerichtshof (VGH) Mannheim verpflichtet, Auskunft auch über die Namen der Schöffen zu erteilen. Im Übrigen, nämlich hinsichtlich der Namen des Vertreters der Staatsanwaltschaft, des Verteidigers und der Urkundsbeamtin wurde die Abweisung der Klage bestätigt: Insoweit überwiege das grundrechtlich geschützte Persönlichkeitsrecht der Betroffenen das ebenfalls grundrechtlich geschützte Auskunftsrecht der Presse.

Ausgangspunkt des Verfahrens war ein Urteil des AG Nürtingen, das auf Antrag der Staatsanwaltschaft ein traumatisiertes Kind aus Afghanistan zu 6 Monaten Haft ohne Bewährung verurteilt hatte, weil es aus dem unsicheren Staat Griechenland mit dem Flugzeug weiter nach Deutschland geflohen war, wo es ein ihm von Schleppern übergebenes Reisedokument auf Aufforderung vorzeigte. Dieselbe Strafe hatte der „Verteidiger" gefordert und sofort nach der Verurteilung Rechtsmittelverzicht erklärt. Das Kind hatte bereits ca. 4 Monate in Untersuchungshaft gesessen, die es weitgehend in einer Klinik des baden-württembergischen Strafvollzugs verbringen musste, wo es mit Medikamenten ruhiggestellt wurde. Die Ausländerbehörde verfügte daraufhin wegen der Verurteilung durch das AG Nürtingen die Ausweisung aus Deutschland. Im verwaltungsgerichtlichen Verfahren wurde die Ausweisungsverfügung aufgehoben und das Urteil des AG Nürtingen kritisiert. Hierüber wurde in der baden-württembergischen Presse berichtet.

Das BVerwG gab der Revision des Klägers hinsichtlich des Anspruchs auf Auskunftserteilung über die Namen des Staatsanwalts und des Verteidigers in dem Strafverfahren statt. Das Persönlichkeitsrecht dieser Personen müsse hinter dem grundrechtlich geschützten Auskunftsinteresse der Presse zurückstehen. Sie stünden kraft des ihnen übertragenen Amtes bzw. ihrer Stellung als Organ der Rechtspflege hinsichtlich ihrer Mitwirkung an Gerichtsverfahren im Blickfeld der Öffentlichkeit. Ein berechtigtes Interesse, ihre Identität nicht gegenüber der Presse preiszugeben, sei angesichts der hohen Bedeutung des Grundsatzes der Öffentlichkeit für ein rechtsstaatliches Gerichtsverfahren nur dann anzunehmen, wenn sie erhebliche Belästigungen oder eine Gefährdung ihrer Sicherheit zu befürchten haben. Letzteres war nach den tatsächlichen Feststellungen des VGHs hier nicht der Fall. Entgegen der Auffassung des VGH lasse sich ein Vorrang ihres Persönlichkeitsrechts nicht mit der Erwägung begründen, sie trügen keine unmittelbare Verantwortung für ein Strafurteil, so dass die Kenntnis ihrer Namen keinen hinreichenden Informationswert für die Presse besitze. Verteidiger und Staatsanwalt nähmen auf den gerichtlichen Verfahrensgang Einfluss. Zudem sei es nicht Sache staatlicher Stellen, sondern der Presse selbst, darüber zu bestimmen, welche Informationen unter welchen Aspekten vonnöten sind, um ein bestimmtes Thema zum Zweck einer möglichen Berichterstattung über Gerichtsverfahren im Recherchewege aufzubereiten. Der Staat habe nicht in eine journalistische Relevanzprüfung einzutreten.

Die Presse darf gemäß dem Urteil des BVerwG im Rahmen der Recherche zu Gerichtsverfahren aber nicht die Namen von Personen herausfordern, denen selbst bei Anlegung eines großzügigen, den besonderen Funktionsbedürfnissen und Arbeitsgewohnheiten der Presse vollauf Rechnung tragenden Maßstabs kein materielle Bedeutung im Zusammenhang mit dem Thema der Recherche bzw. der ins Auge gefassten Berichterstattung zukommt. Erfolglos bleiben müssten also Informationsverlangen „ins Blaue" hinein, bei denen kein ernsthafter sachlicher Hintergrund besteht. Verweigert eine staatliche Stelle aus diesen Gründen die Herausgabe einer personenbezogenen Information und erläutert die Presse daraufhin nicht zumindest ansatzweise den von ihr zugrunde gelegten Wert dieser Information für ihre Recherche bzw. die ins Auge gefasste Berichterstattung, kann die staatliche Stelle das Informationsverlangen mangels ernsthaftem Hintergrund ausnahmsweise verweigern. Deshalb hat das BVerwG die Revision zurückgewiesen, soweit sie das Verlangen nach Bekanntgabe des Namens der Urkundsbeamtin betraf (BVerwG PE Nr. 57/2014 v. 01.10.2014; Mitteilung des klagenden Anwaltes v. 02.10.2014).

BVerwG

Kein Eingriff bei bayerischer automatisierter Kennzeichenerfassung

Das Bundesverwaltungsgericht (BVerwG) in Leipzig hat mit Urteil vom 22.10.2014 eine Klage abgewiesen, die

dem Freistaat Bayern verbieten wollte, durch den verdeckten Einsatz automatisierter Kennzeichenerkennungssysteme die Kraftfahrzeuge (Kfz) des Klägers zu erfassen und mit polizeilichen Dateien abzugleichen (6 C 7.13).

Der beklagte Freistaat Bayern setzt seit 2006 stationäre und mobile Kennzeichenerfassungsgeräte ein. Die stationären Geräte sind derzeit auf zwölf Standorte insbesondere an den bayerischen Autobahnen verteilt. Die mobilen Geräte werden aufgrund der jeweiligen Lagebeurteilung des Landeskriminalamtes (LKA) anlassbezogen, beispielsweise bei internationalen Fußballturnieren oder ähnlichen Großveranstaltungen, eingesetzt. Die stationären Anlagen bestehen aus einer Kamera, die den fließenden Verkehr auf jeweils einer Fahrspur von hinten erfasst und das Kennzeichen eines jeden durchfahrenden Fahrzeugs mittels eines nicht sichtbaren Infrarotblitzes aufnimmt. Aus dem digitalen Bild des Kennzeichens wird durch eine spezielle Software ein digitaler Datensatz mit den Ziffern und Buchstaben des Kennzeichens ausgelesen und über eine Datenleitung an einen stationären Rechner weitergeleitet, der am Fahrbahnrand in einem verschlossenen Behälter untergebracht ist. Dort wird das erfasste Kennzeichen mit verschiedenen im Rechner gespeicherten Fahndungsdateien abgeglichen. Bei mobilen Anlagen werden die Kennzeichen über am Fahrbahnrand aufgestellte Kameras erfasst und über einen mobilen Rechner in einem vor Ort abgestellten Polizeifahrzeug mit den Fahndungsdateien abgeglichen.

Geklagt hatte der Informatiker Benjamin Erhart, weil die Erfassung Millionen Autofahrer unter Generalverdacht stelle. Autofahrer könnten durch den „fehleranfälligen Massenabgleich“ irrtümlich angehalten und kontrolliert werden. Es sei auch nicht ausgeschlossen, dass Polizei und Geheimdienste Bewegungsprofile erstellten. Die Maßnahme habe „abschreckende Wirkung“ auf die Gesellschaft und keinen nennenswerten Nutzen. Die Erfolgsquote liegt Erhart zufolge bei 0,03%. Er wohnt in Bayern mit einem weiteren Wohnsitz in Österreich und ist nach seinen Angaben häufig in Bayern mit seinem Kfz unterwegs. Er beantragte mit seiner Klage, die Erfassung und den Abgleich seiner Kfz-Kennzeichen zu unterlassen. Der automatisierte Abgleich seiner Kfz-Kennzeichen beeinträchtige sein allgemeines Persönlichkeitsrecht und greife in sein Grundrecht auf informationelle Selbstbestimmung ein. Das Verwaltungsgericht München hatte die Klage am 23.09.2009 abgewiesen (M 7 K 08.3052), der Verwaltungsgerichtshof (VGH) München hatte die Berufung des Klägers am 17.12.2012 (10 BV 09.2641) zurückgewiesen.

Das BVerwG wies die Revision des Klägers zurück. Es wies die Unterlassungsklage zurück, weil dem Kläger durch die Anwendung der gesetzlichen Vorschriften über die automatisierte Kennzeichenerfassung mit hinreichender Wahrscheinlichkeit kein Eingriff in sein grundrechtlich geschütztes Recht auf informationelle Selbstbestimmung als Unterfall des allgemeinen Persönlichkeitsrechts drohe. Gemäß den tatsächlichen Feststellungen des VGH, an die das BVerwG als Revisionsgericht gebunden ist, wird das Kennzeichen eines vorbeifahrenden Kfz von dem Gerät erfasst und mit den dafür herangezogenen Dateien abgeglichen. Wenn keine Übereinstimmung mit Kennzeichen in den Dateien festgestellt wird, liege kein Eingriff in das Recht auf informationelle Selbstbestimmung vor. In diesem Fall sei rechtlich und technisch gesichert, dass die Daten anonym bleiben und sofort spurenlos und ohne die Möglichkeit, einen Personenbezug herzustellen, gelöscht werden. Ebenso wenig liege ein Eingriff in den Fällen vor, in denen ein Kennzeichen von dem Gerät erfasst und bei dem Abgleich mit den Dateien eine Übereinstimmung mit Kennzeichen in den Dateien angezeigt wird, der sodann vorgenommene manuelle Vergleich von abgelichtetem Kennzeichen und dem vom System ausgelesenen Kennzeichen durch einen Polizeibeamten aber ergibt, dass die Kennzeichen tatsächlich nicht übereinstimmen. In diesem Fall lösche der Polizeibeamte den gesamten Vorgang umgehend durch Eingabe des Befehls „Entfernen“, ohne dass er die Identität des Halters ermittelt. Ein Eingriff liege nur vor, wenn das Kennzeichen von dem Gerät erfasst wird und bei dem Abgleich mit den Dateien eine Übereinstimmung mit Kennzeichen in den Dateien angezeigt wird, die tatsächlich gegeben ist. In diesem Fall wird der Vorgang gespeichert und steht für weitere polizeiliche Maßnahmen zur Verfügung. Dem Kläger drohe ein solcher Eingriff jedoch nicht mit hinreichender Wahrscheinlichkeit, weil die Kennzeichen von ihm gehaltener Kraftfahrzeuge nicht in den herangezogenen Dateien gespeichert sind und nur eine hypothetische Möglichkeit dafür besteht, dass sie künftig dort gespeichert werden könnten. Vertreten wurde Erhart von Udo Kauß. Der Freiburger Jurist hatte 2008 Verfassungsbeschwerden gegen das Kfz-Kennzeichen-Scanning in Hessen und Schleswig-Holstein erfolgreich durchgefochten. Nun soll auch die bayerische Vorgehensweise vom Bundesverfassungsgericht geprüft werden (BVerwG PM v. 22.10.2014, Klage gegen automatisierte Kennzeichenerfassung in Bayern erfolglos; Krempl, www.heise.de 23.10.2014).

OVG Schleswig-Holstein

Fanpagebetreiber für Nutzungsdatenverarbeitung Facebooks nicht verantwortlich

Mit Urteil vom 04.09.2014 entschied das Schleswig-Holsteinische Oberverwaltungsgericht (OVG), dass Betreiber von Facebook-Fanpages in keiner Weise eine Verantwortung für die hierüber ausgelöste Verarbeitung von Nutzungsdaten bei Facebook tragen (4 LB 20/13). Sie seien weder verantwortliche Stelle im Sinne des Datenschutzrechts noch als Störer verantwortlich zu machen. Hintergrund des Urteils ist eine Musterverfügung, mit der das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) der Wirtschaftsakademie der Industrie- und Handelskammer (WAK) auferlegt hatte, ihre Fanpage bei Facebook zu deaktivieren. Begründet wurde dies vom ULD mit datenschutzrechtlichen Verstößen von Facebook – insbesondere einer fehlenden Widerspruchsmöglichkeit von Nutzern nach dem Telemediengesetz gegen die Erstellung von Nutzungsprofilen. Hiergegen hatte die WAK erfolgreich beim Verwal-

tungsgericht Schleswig (VG) geklagt.

Mit dem Urteil wurde die Berufung des ULD gegen das Urteil des VG vom 09.10.2013 (DANA 4/2013, 169) vom OVG zurückgewiesen. Der vorsitzende Richter verwies Betroffene wie auch Aufsichtsbehörden darauf, sich wegen Datenschutzverstößen an Facebook zu halten, wobei während der Verhandlung nicht geklärt wurde, ob dies Facebook Inc. in den USA, Facebook Ltd. in Dublin/Irland oder Facebook Germany in Hamburg sei. Obwohl die Betreiber von Fanpages die Datenverarbeitung durch Facebook auslösen, kann es diesen, so die Schlussfolgerung des ULD, völlig egal sein, ob die Datenverarbeitung durch Facebook in rechtmäßiger oder rechtswidriger Weise geschieht. Das OVG begründete dies damit, dass die Fanpagebetreiber keinen Einfluss auf die technische und rechtliche Ausgestaltung der Datenverarbeitung durch Facebook hätten. Nach Auffassung des OVG war die Anordnung des ULD auch rechtswidrig, weil vor einer Untersagungsverfügung an einen datenschutzrechtlich Verantwortlichen erst ein abgestuftes Verfahren einzuhalten sei, in dem zunächst eine Umgestaltung der Datenverarbeitung angeordnet und ein Zwangsgeld verhängt werden muss. Eine rechtlich grundsätzlich denkbare Ausnahmesituation hiervon habe hier nicht vorgelegen.

Marcus Schween, Federführer Recht der IHK Schleswig-Holstein, sah sich mit dem Urteil bestätigt: „Auch schleswig-holsteinische Unternehmen können, wie alle anderen Unternehmen in Deutschland und Europa, soziale Netzwerke wie Facebook als Kommunikations- und Vertriebskanal nutzen. Mit diesem Urteil sind Drohungen gegenüber Unternehmen oder Behauptungen, Unternehmen würden sich rechtswidrig verhalten, nun endgültig der Boden entzogen.“ Es sei ein hohes Maß an Rechtssicherheit hergestellt worden. „Ich gehe auch davon aus, dass das ULD sich zukünftig im Ton mäßigt, wenn es sich zur Verwendung von Fanpages äußert.“ Thilo Weichert, Leiter des ULD, zeigte sich von dem Urteil schwer enttäuscht: „Das zentrale Argument des ULD, dass das Betreiben einer Fanpage ein rechtlich und technisch einheitlicher Vorgang ist, bei dem sich Betreiber und Facebook gegenseitig ergänzen und voneinander abhängig sind, wurde nicht gewürdigt. Die Botschaft des Urteils gibt behördlichen oder kommerziellen Seitenbetreibern auf illegalen Portalen aus den USA wie z. B. Facebook zwar vorläufig Rechtssicherheit, lässt aber die User als Betroffene im Regen stehen – eine Katastrophe und ein Rückschlag für den Datenschutz. Hat dieses Urteil Bestand, so bleibt der Verantwortungslosigkeit im Internet Tür und Tor geöffnet.“ Weichert kündigte an, gegen das Urteil vor dem Bundesverwaltungsgericht Revision einzulegen, wo klargestellt werden müsse, „dass sich Institutionen ihrer datenschutzrechtlichen Verantwortung nicht dadurch entziehen können, dass sie Dritte mit illegaler Datenverarbeitung beauftragen“ (ULD PM v. 29.09.2014, „OVG-Urteil zu Facebook-Fanpages revisionsbedürftig“; ULD PM v. 05.09.2014, Schleswig-Holsteinisches OVG: Rechtssicherheit für Betreiber – nicht für die Betroffenen; IHK Schleswig-Holstein, Medieninformation v. 04.09.2014, Es bleibt dabei: Fanseiten sind zulässig!; OVG Schleswig PM v. 05.09.2014: Wirtschaftsakademie kann vom ULD nicht zur Abschaltung ihrer Facebook-Fanpage verpflichtet werden).

LG München I

Spannerfotos sind keine Straftat

Ein ehemaliger Bürgermeister des bayerischen Ortes Scheyern im Landkreis Pfaffenhofen fotografierte jungen Frauen unter den Rock und erstellte so mindestens 99 Bilder und 27 Videos. Das Landgericht (LG) München I entschied am 17.09.2014, dass es sich dabei aber nicht um eine Straftat handele, sondern nur um eine Ordnungswidrigkeit. Der 56-Jährige muss dennoch eine Geldstrafe zahlen, weil er sich bei seiner Festnahme gewehrt hatte. Die Bilder entstanden heimlich im Sommer 2013 am Münchner Stachus auf einer Rolltreppe. Der Verkäufer einer Obdachlosenzeitung hatte dies beobachtet und rief die Polizei. Im März 2014 war der Spanner dafür vom Amtsgericht zu einer Geldstrafe von 5.250 Euro verurteilt worden (DANA 2/2014, 77 f.). Dagegen hatte er Berufung eingelegt und nun teilweise Recht bekommen. Das LG sah keinen Tatbestand der Beleidigung bei der Spanner-Aktion, so Richterin Elisabeth Ehrl: „Man muss sich jeden Einzelfall anschauen. Man müsste entweder einen neuen Paragrafen schaffen oder den Beleidigungsparagrafen anders fassen.“ Weil sich der Spanner bei seiner Festnahme gewehrt und einen Polizisten verletzt hatte, wurde er zu 4200 Euro Strafe verurteilt, plus 750 Euro Bußgeld für die Belästigung der Allgemeinheit (Gericht hält Spannerfotos nicht für Straftat, www.sueddeutsche.de 18.09.2014; Gericht: Spannerfotos sind keine Straftat, SZ 19.09.2014, 45).

VG Köln

BfV muss Gysi-Akten löschen

Mit einem Anerkenntnisurteil vom 21.08.2014 hat das Verwaltungsgericht (VG) Köln das Bundesamt für Verfassungsschutz (BfV) verpflichtet, die Personenakte des Linken-Fraktionschef im Bundestag Dr. Gregor Gysi zu vernichten bzw. diejenigen Daten zu löschen, die elektronisch gespeichert wurden (20 K 1468/08). Seit 2006/2007 stritten Gysi und das BfV um die Löschung und Vernichtung der personenbezogener Daten des Klägers. Nachdem das Bundesverfassungsgericht mit Beschluss vom 17.09.2013 (2 BvR 2436.10 und 2 BvE 6.08, „Fall Ramelow“, DANA 1/2014, 45 f.) entschieden hatte, dass die langjährige Beobachtung dieses ehemaligen Bundestags- und jetzigen Landtagsabgeordneten für die Partei Die Linke einen Eingriff in dessen freie Mandatsausübung darstelle und nicht gerechtfertigt sei, erklärte das BfV, dass es nunmehr auch die gespeicherten Daten des Klägers löschen bzw. vernichten werde, worauf das VG auf Antrag des Klägers ein entsprechendes Anerkenntnisurteil erließ. Gysi zeigte sich erfreut über die Entscheidung und forderte eine grundsätzliches Ende der Beobachtung der Linken: „Der Verfassungsschutz hat auf ganzer Linie verloren“ (PE VG Köln 05.09.2014, Bundesamt für Verfassungsschutz muss „Gysi-Akten“ löschen; SZ 06./07.09.2014, 6).

Buchbesprechungen

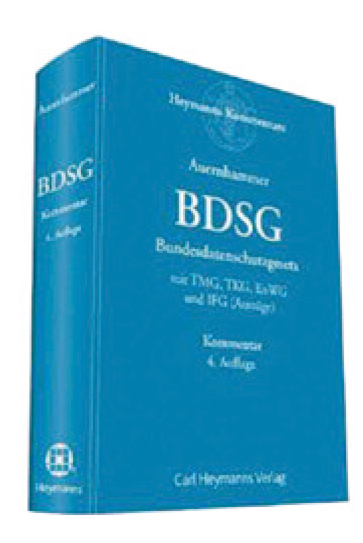


Markus Morgenroth
Sie kennen dich! Sie haben dich! Sie steuern dich!
Die wahre Macht der Datensammler
Droemer München, 2014, 271 S., ISBN 978-3-426-27646-4

(tw) Es kann inzwischen in tausenden Artikel nachgelesen werden, wie private Unternehmen mit welchen technischen Methoden und welchen mehr oder weniger falschen Versprechungen und Behauptungen Menschen verdaten. Der Autor Morgenroth fasst in seinem Buch diese versprengten Erkenntnisse (mit Internet-Quellennachweisen) aktuell in einem Buch zusammen und ergänzt diese mit eigenen Erfahrungen. Diese stammen aus seiner Tätigkeit als Softwareingenieur für ein Unternehmen im Bereich der verhaltensbasierten Datenanalyse im Silicon Valley. 2007 bis 2013 leitete er die europäische Niederlassung von Cataphora. Danach stieg er aus und berät seitdem Unternehmen wie BürgerInnen über die Möglichkeiten und Risiken von Big Data sowie zum Datenschutz.

Sein Buch ist eine Rundreise durch die stark von US-Unternehmen beeinflusste und dominierte Welt der wirtschaftlich motivierten Datenerfassung und -analyse von VerbraucherInnen, Beschäftigten oder einfach Internet-Nutzenden. Bei dieser Tour werden die Unternehmen und ihre Praktiken genannt: von Microsoft, Google, Facebook, Apple, Acxiom, Twitter, WhatsApp, Amazon, eBay, MEDBase200 .... bis hin zu Bertelsmann, Otto, Post, Schober, AZ Direkt, Arvato Infoscore, Schufa, Ikea, Creditreform, Payback, AXA, SAP, Zalando ... Er zeigt präzise auf, mit welchen Mitteln – Video, Funktechnik, Mail, Kunden- und Mitgliedskarten, Smartphones, Apps, Internet-PCs, eBook, Online-Spiele, soziale Netzwerke, Wearables ... die Daten gesammelt und wie diese über digitale Auswertungen – von Scoring, Tracking, Profiling bis Big Data – für Zwecke der Kontrolle, der Manipulation und der Diskriminierung genutzt werden. Selbst sensibelste Gesundheitsdaten sind kein Tabu. Er beschreibt, wie der Algorithmus an die Stelle des Personalchefs, des Marketingspezialisten und des Kreditsachbearbeiter tritt. Dies erfolgt nicht nur abstrakt, sondern an Hand von vielen lebendigen Beispielen.

Er räumt mit der Hoffnung auf Anonymität, auf Vertrauen und Vertraulichkeit, auf Unbeobachtetheit und das Verschwinden in der Menge auf. Er stellt klar, dass Metadaten höchst sensibel sein können. Er zeigt auf, wie Stalker und Cyerkriminelle ein leichtes Spiel haben. Gesetzliche Datenschutzregeln spielen keine Rolle, wenn mit den Gesetzesverstößen Geld verdient werden kann. Dabei spart der Autor keinen Lebensbereich aus: von der Auskunftei über Auto und Arbeitsplatz, Finanzdienstleistung, Handel, Internet, Television bis zu Versicherung Am Ende gibt er knappe und gute Tipps zum Weiterlesen im Netz.



Auernhammer, Hrsg. Eßer, Martin/Kramer, Philipp/von Lewinski, Kai
BDSG – Bundesdatenschutzgesetz und Nebengesetze
Kommentar
Carl Heymanns Verlag, Köln, 4. Aufl. 2014
ISBN 978-3-452-27574-5

(tw) Wer die Qualität des Datenschutzes eines Landes an der Zahl der Kommentare zum nationalen Datenschutzrecht misst, muss zu dem Ergebnis kommen, dass wir in Deutschland einen hohen Standard haben. Kurz bevor sich das nationale Datenschutzrecht abzumelden scheint, um einer Europäischen Datenschutz-Grundverordnung (EU-DSGVO) Platz zu machen, erscheinen neue Kommentare. Neuer Kommentar? Auernhammer war der erste Kommentar 1977 nach der erstmaligen Verabschiedung des BDSG im Jahr 1976. Seine bisher letzte, 3. Auflage erschien nach der ersten umfassenden BDSG-Novellierung im Jahr 1993. Doch hat der neue Auernhammer mit den vorherigen außer dem Namen und dem Verlag nichts mehr gemein. Herbert Auernhammer,

ein Ministerialbeamter der ersten Stunde des Datenschutzes müsste wohl zugestehen, dass sich in den letzten 20 Jahren Einiges getan hat.

Eine zentrale Verantwortung für den Kommentar hat offensichtlich Kai von Lewinski übernommen, der nicht nur viele Einzelparagrafen kommentiert, sondern auch Grundsatzerwägungen insbesondere in der Einleitung präsentiert. Diese sind für jemanden, der eine demokratisches und gesellschaftlich orientiertes Verständnis von Datenschutz hat, wenig erquickend. Schon in Rdn. 2 behauptet er: „Datenschutz ist nicht nur Vorfeldschutz, sondern beschreibt eine ganze Vorfeldschutz-Kaskade. Zum eigentlichen Schutzgut des BDSG erklärt er den Eigenwert des Menschen und seine Psyche, wobei „das Recht dabei (potentiell und auch praktisch) immer unschärfer und ggf. sogar dysfunktional“ werde (Rdn. 3). Was das Bundesverfassungsgericht (BVerfG) als „informationelle Selbstbestimmung“ gekennzeichnet hat, würde von Lewinski lieber präziser mit „informationeller Fremdbestimmung“ beschreiben (Rdn. 10). Bei den Datenschutzgesetzen der Siebziger und Achtziger Jahre handele es sich um einen „realtiv seltenen Fall vorauseilender Gesetzgebung, also um Gesetzgebung vor dem Akutwerden des Problems“ (Rdn. 21). Dem muss man nicht nur widersprechen, wenn man in den 80er Jahren – angesichts der Überwachungserfahrungen im Nationalsozialismus – gegen Volkszählungen protestierte und angesichts der Sicherheitsgesetze eines Innenministers Friedrich Zimmermann sich um die Freiheitlichkeit unserer Gesellschaft sorgte. Des Autoren reduziertes Verständnis von Datenschutz zeigt sich auch in seiner Behauptung, das Grundgesetz schreibe „kein institutionelles System des Datenschutzes“ fest (Rdn. 64), womit er sich nicht nur in Widerspruch zum BVerfG setzt. Entgegen der öffentlichen Meinung behauptet von Lewinski schließlich, dass das Datenschutzrecht „mit dem BDSG von einem undurchsichtigen Gesetz geregelt (werde), das mit dem Verbot mit Erlaubnisvorbehalt ein in der Informationsgesellschaft nur schwer vermittelbares Regelungskonzept verfolgt“ (§ 38a Rdn. 1).

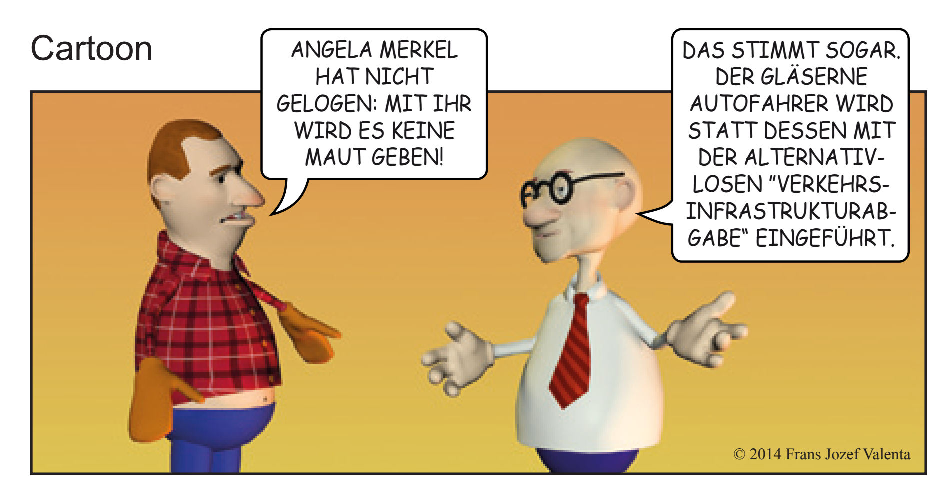
Derart ideologisch vorbelastet erweist sich der vorliegende Kommentar insgesamt dann aber praktisch als ein eher positiv zu bewertendes Unterfangen: Die von von Lewinski vorgegebenen Grundsatzerwägungen finden sich in den Einzelkommentierungen nicht wieder. Diese entsprechen vielmehr den praktischen Erfordernissen und belegen, dass das Regelungskonzept des BDSG doch vermittelbar ist. Tatsächlich verfolgen – ebenso wie bei den meisten BDSG-Kommentaren – die AutorInnen keine einheitlichen Linien oder Interessen, es gibt eher grundrechts- und eher verarbeitungsfreundliche Beiträge. Die Autorinnen kommen aus allen Bereichen: der Verwaltung (Eßer, Greve, Meints, Onstein, Raum), der Rechtsanwaltschaft (Heun, Kramer, Schimanek, Schreibauer), der Privatwirtschaft (Stollhoff, Thomale), dem Presserat (Führ) und der Wissenschaft (Forst, Herbst, Hornung, von Lewinski). Sämtliche zeichnen sich durch eine aktuelle und valide Bearbeitung der vorhandenen Literatur aus, wobei Praktikerbedürfnissen eher entsprochen wird als wissenschaftlichen Ansprüchen. Dessen ungeachtet werden Meinungsunterschiede dargestellt und bewertet, wenngleich zumeist nicht intensiv diskutiert.

Üblich gut ist die Literaturübersicht. Die besondere Brauchbarkeit des Kommentars hebt sich durch einige Eigenschaften hervor: Kommentiert werden nicht nur die Normen des BDSG, sondern auch Datenschutzregelungen des TKG (§§ 88-115), des TMG (§§ 11-15), des IFG Bund (§ 5) und des EnWG (§§ 21g, 21h). Den einzelnen Kommentierungen sind die Regelungen der europäischen Datenschutzrichtlinie und deren Erwägungsgründe vorangestellt. Die Google-Entscheidung des EuGH vom 13.05.2014 wurde noch mitberücksichtigt. In allen Regelungen wird auch die Planungsperspektive der EU-DSGVO angesprochen.

Die Diskussion wird auf der Höhe der Zeit, der aktuellen Techniken und Konflikte geführt. Damit folgt der Kommentar praktisch allen Angeboten auf dem Markt, die sich durch gediegene Darstellung mehr als – abgesehen von der oben dargestellten Position von Lewinskis – durch besondere Originalität auszeichnen. So wäre etwa eine Darstellung der Debatte um Schutzziele nicht schädlich gewesen. Auch die Erörterung des Konfliktes zwischen Meinungsfreiheit und Persönlichkeitsschutz bewegt sich im Bereich des Üblichen.

Sehr zu begrüßen ist, dass einige relevante Datenschutznebengesetze (insbes. TKG, TMG) mitkommentiert sind. Von hohem praktischen Gebrauchswert sind auch die vielen Anhänge, die einen veranlassen können, das mit seinen 2000 Seiten dennoch handliche Buch immer wieder zu Rate zu ziehen: Dort finden sich das gesamte IFG-Bund, Auszüge aus dem StGB, dem BBG, dem UWG, dem SGB I und X, der AO, der BRAO, die TKÜV, sowie auf europäischer Ebene die EU-Datenschutzverordnung von die EU selbst, die Telekommunikationsrichtlinie, das Europarats-Übereinkommen sowie die Vorschläge der Kommission zur EU-DSGVO sowie zur Richtlinie für den Bereich der Verhütung und Verfolgung von Straftaten und schließlich die Satzung der Stiftung Datenschutz (was wohl weniger von praktischer Relevanz ist). Das Stichwortverzeichnis ist von wünschenswerter Ausführlichkeit.

Cartoon



Hol Dir Deinen kostenlosen Peilsender!



Du hast irrsinnig viele Modelle zur Auswahl

FESTNETZ ✓ **FLATRATE**

ALLE MOBILFUNK-NETZE ✓ **FLATRATE**

INTERNET ✓ **FLATRATE**



*) Inklusive kostenfreiem Ortungsservice